查询DS2050W供应商



DS1963S
SHA iButton

www.iButton.com

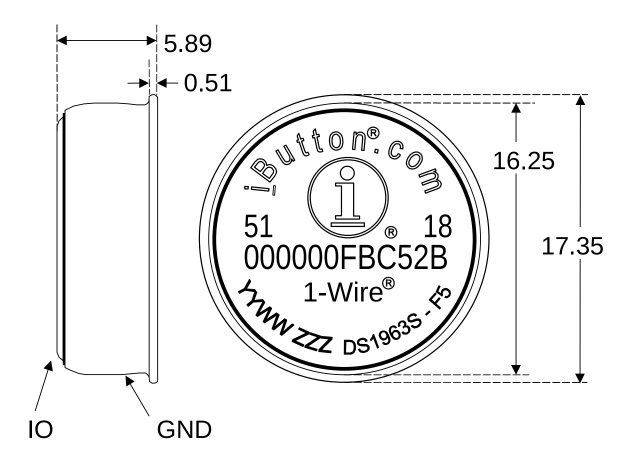
特性

- 4096 位可读/写非易失（NV）存储器，分为 16 页，每页 256 位
- 8 个存储页分别具有独立的 64 位密钥和 32 位只读、不滚动、页写计数器
- 密钥只可写入，并具有自己独立的写循环计数器
- 片内 512 位 SHA-1 (FIPS 180-1，ISO/IEC 10118-3) 引擎可计算 160 位信息鉴定码（MAC），生成页密钥
- 器件可作为漫游iButton®或主机的协处理器使用
- 256 位暂存器保证传送数据的完整性
- 片内 16 位 CRC 发生器确保数据正确传送
- 高速模式提升通信速度至 125kbps
- 工作温度范围-20°C 至+85°C
- 数据保留 10 年以上

iButton的共性

- 唯一的、经工厂光刻和测试的 64 位注册码（8 位家族码 + 48 位序列码 + 8 位 CRC 校验码）保证绝对可溯性，因为没有任何两个器件是相同的
- MicroLAN 多点控制器
- 通过瞬间接触完成数字识别和信息传递
- 基于芯片的数据载体实现信息的紧凑存储
- 可附着在目标物体上读取数据
- 通过一条信号线与主机通信，速率达 15.4kbps，极为经济
- 标准 16mm直径，使用 1-Wire®协议，保证与其它iButton系列器件兼容
- 钮扣外形，可自动对准杯状探头
- 坚固的不锈钢外壳，表面铭刻注册码，可抵御恶劣工作环境
- 便于安装，可用自粘胶、固定凸缘、或在边缘嵌装箍环等办法安装
- 当阅读器首次上电时进行在线检测应答
- 符合 UL#913 (第四版)标准；本质安全器件，经过 I 级，1 区，A、B、C、D 组指定区域的认证（申请中）

F5 MicroCan



图中尺寸均以毫米为单位

定购信息

DS1963S	F5 MicroCan

相关产品

DS9096P	自粘胶垫
DS9101	多用途夹
DS9093RA	安装固定环
DS9093A	链扣
DS9092	iButton读取探头

iButton 和 1-Wire 是 Dallas Semiconductor的注册商标。

iButton 概述

DS1963S是一个带有SHA-1 功能和 4k位读/写数据区的金融iButton，通过简单硬件就可完成数据读写。它的非易失存储器可根据需要建立公用数据和器件持有者或应用环境的私有数据微数据库。其片内的 512 位SHA-1 引擎可根据器件内部存储的信息计算 160 位信息鉴定码（MAC）。数据通过 1-Wire协议串行传送，仅需一条信号线和地线。采用TMEX文件格式（参见应用笔记 114），单一DS1963S可被用于四个相互独立的应用，例如作为安全电子钱包为本地运输系统、付费电话、停车管理、售货机等应用提供电子支付手段。另外，DS1963S也可作为一个协处理器协助主机计算签名，以便在消费结束后，利用一个安全签名密钥，将新的余额写回漫游装置。

与其他基于SRAM的iButton一样，DS1963S也具有一个附加的存储区域，称为暂存器，在对主存储器进行写操作时可作为一个缓冲器使用。DS1963 的暂存器也被用于向SHA-1 引擎提供数据，或者接收/比较信息鉴定码。

在进行写操作时，数据首先被写入暂存器，并可以从这里读回数据进行核对。数据经过核对之后，一条 Copy Scratchpad（复制暂存器）命令就可将数据传送到主存储器。这种处理方式保证了在不可靠接触条件下写入主存储器数据的完整性。

每个 DS1963S 都在出厂时都写入了一个 64 位 ROM 注册码，这个唯一的 ID 确保每个器件都绝对可溯。坚固耐用的 MicroCan 封装保证器件具有很高的防污、防潮和抗冲击性能。DS1963S 紧凑的钮扣外形可自动对准与之相配套的读写头，使用者操作起来非常容易。各种附件使 DS1963S 可以安装在塑料钥匙扣、证件和印制电路板等各种物体的表面上。

安全性

使用移动数据载体的系统主要由 3 部分组成：1）读、写数据载体的主机；2）数据载体（“从设备”）；3）系统的使用者（使用者有可能会试图篡改数据或假造数据载体）。DS1963S 专门设计用于抵御对所有这些环节的攻击，并且没有使用任何有产权限制的算法。该器件的安全性基于安全散列标准 SHA-1（Secure Hash Standard），相关文档参见 http://www.itl.nist.gov/div897/pubs/fip180-1.htm。

下表以真值表的形式列出了各种可能的非暴力攻击手段。表中涉及的注解解释了防范这些攻击的典型方法。关于其中所用到的功能的完整描述详见“存储器和 SHA 功能命令”章节及 SHA-1 算法和信息格式。

	可信数据	伪造数据	
授权主机	见注释 2	见注释 2、3	假从机
授权主机	正常操作	见注释 3	可信从机
非授权主机	见注释 1	不考虑	可信从机
非授权主机	不考虑	不考虑	假从机

注释 1: 基于保存在漫游数据载体存储页中的系统级密钥、器件 ROM 注册号和用户选定的用户密码，器件可被用于主机的鉴定。

注释 2: 为了确认从设备的可信度，主机向暂存器写入一个 3 字节的“质询”，然后发出命令令其针对质询、某存储页的数据、页号、该页的写循环计数器、设备的 ROM 注册码、以及和该页相关的密钥计算 SHA-1 MAC。通过每次变换由从机读出的质询，主机可以确认从机是否拥有正确的密钥，并在要求的时间内完成 SHA 计算。

注释 3: 如果数据在从机内被授权主机“签署”，伪造数据就能被发现。签署时需要计算一个 160 位的 SHA-1 MAC，计算过程涉及被保护数据、数据所在页的写循环计数器、存储数据的从设备的 ROM ID，以及任何只有授权主机知晓的专用密钥。MAC 和应用数据（例如货币数值和交易 ID 号）一同存放在特定的存储页。要验证数据的可信度，主机可重复签署过程。任何数据，循环计数器，数据载体的改变或使用无效（不属于该系统）的签署密钥都会导致签名验证失败。

概述

图 1 所示为DS1963S的主控和存储单元间的关系。DS1963S有 6 个主要的数据部件：1）64 位光刻 ROM，2）256 位暂存器，3）8 个 32 字节通用SRAM页，4）8 个受写循环计数器保护的 32 字节 SRAM页，5）保存着八个 64 位密钥（每个密钥具有独立的写循环计数器）的两个 32 字节页以及，6）一个 512 位SHA-1 引擎（SHA = 安全散列算法）。图 2 为 1-Wire总线协议的分层结构。全部写循环计数器都为 32 位长，并且到达最大计数后不再滚动。计数器的内容可使用特定命令和内存数据一起被读出。总线主控制器必须首先发出以下 7 条ROM功能命令之一，1）Read ROM（读ROM），2）Match ROM（匹配ROM），3）Search ROM（搜索ROM），4）Skip ROM（跳过ROM），5）Resume Communication（恢复通信），6）Overdrive-Skip ROM（高速跳过ROM）或 7）Overdrive-Match ROM（高速匹配ROM）。以标准速度完成一条Overdrive ROM命令后，器件将进入高速模式（Overdrive mode），接下来的通信将以较高的速度进行。这些ROM功能命令所要求的协议见图 10 所示。成功运行完一条ROM功能命令后，便可进入存储器功能的执行，主机可运行 8 条存储器功能命令的任意一条。这些存储器功能命令的流程参见图 7 所示。全部数据的读和写都为低位先、高位后。

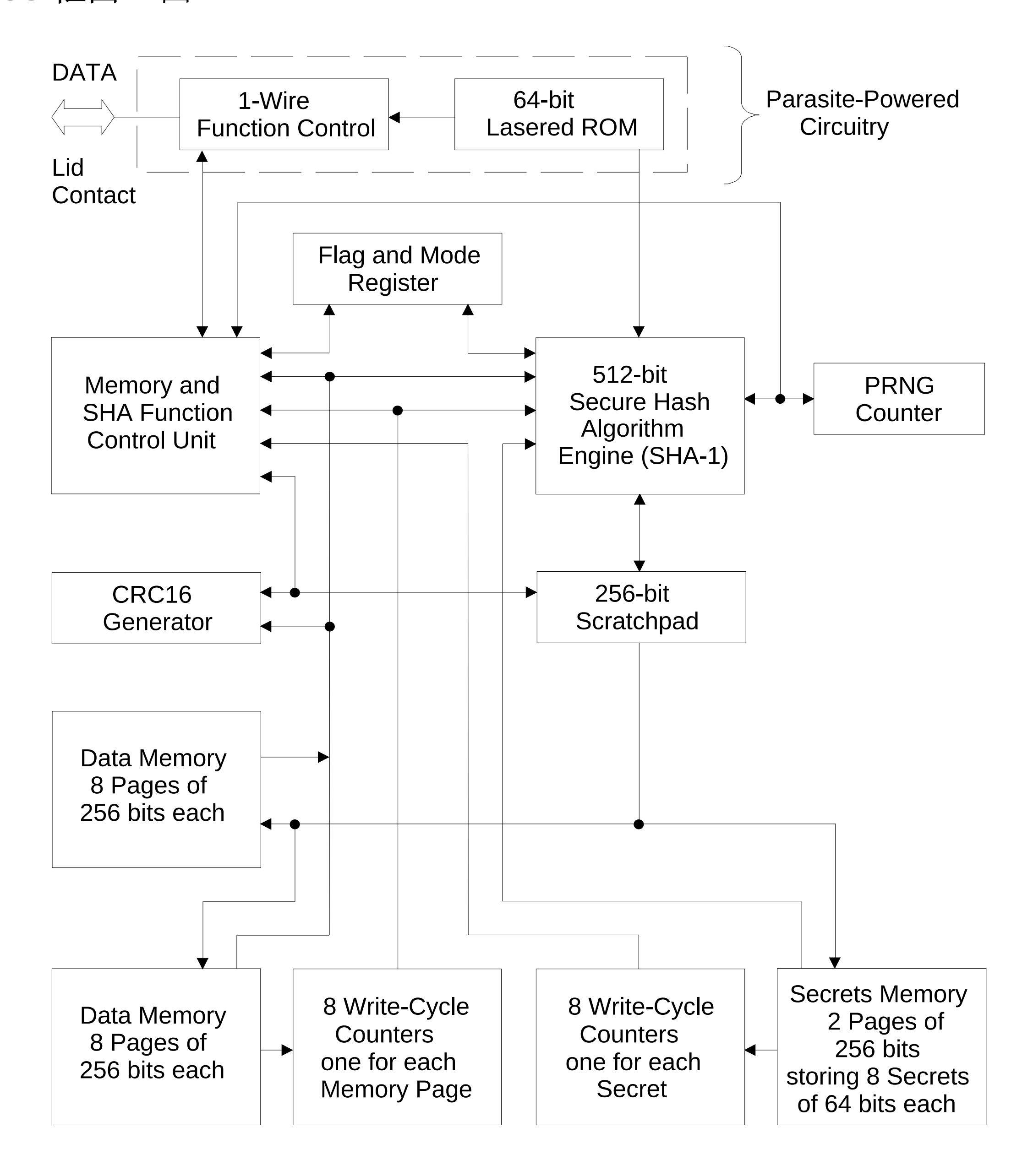
寄生供电

下列框图（图 1）为寄生供电原理电路。该电路在数据触点为逻辑高时“窃取”能量。只要遵守规定的定时和电压要求，所窃得的能量就足以满足数据线为逻辑低状态时电路的需要。寄生供电有两方面的优点：1）通过从输入端获取能量，节省了 DS1963S 内部的锂电池；2）如果某种原因导致锂电池耗尽，仍然可以正常读取 ROM。DS1963S 的其余电路则只能由锂电池提供能量。

64 位光刻 ROM

每个DS1963S具有一个 64 位长的特有ROM码。前 8 位是 1-Wire家族码。接着是 48 位的唯一序列号。最后 8 位是前 56 位的CRC校验码（见图 3）。如图 4 所示，1-Wire CRC由移位寄存器和异或门组成的生成多项式产生。多项式表示为$X^8 + X^5 + X^4 + 1$。关于Dallas的 1-Wire循环冗余校验参见*Book of DS19xx iButton Standards*。移位寄存器初值为零。然后，从家族码的最低位开始，一次移入一位。家族码的第 8 位移入后，开始移入序列号。第 48 位序列号移完后，移位寄存器的值就是CRC码。如果再移入 8 位CRC，移位寄存器应恢复为全零。

DS1963S 框图　图 1



1-Wire 协议的层次结构 图 2

Bus Master

1-Wire Bus

Other Devices

DS1963S

Command Level

1-Wire ROM Function Commands (see Figure 10)

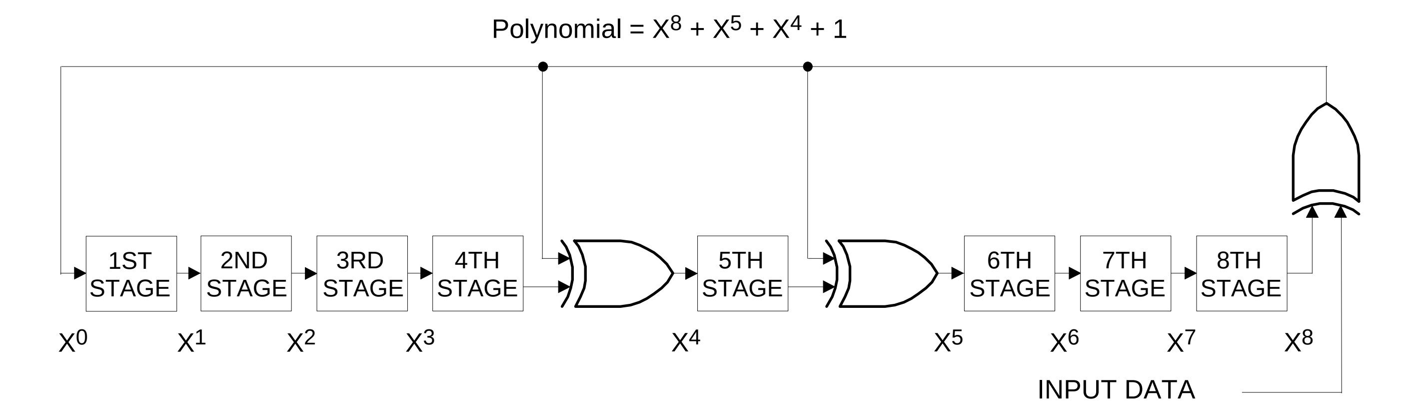
DS1963S specific Memory Function Commands (see Figure 7)

Available Commands	Data Fields Affected
Read ROM	64-bit ROM, RC-Flag
Match ROM	64-bit ROM, RC-Flag
Search ROM	64-bit ROM, RC-Flag
Skip ROM	RC-Flag
Resume	RC-Flag
Overdrive Skip	64-bit ROM, RC-Flag, OD-Flag
Overdrive Match	64-bit ROM, RC-Flag, OD-Flag
Write Scratchpad	256-bit Scratchpad, Flags
Read Scratchpad	256-bit Scratchpad, HIDE Flag
Copy Scratchpad	Data Memory, Secrets Memory, W/C Counter, Flags
Match Scratchpad	160 bits of Scratchpad, Flags
Erase Scratchpad	256-bit Scratchpad, Flags
Read Memory	Data Memory, Flags
Read Authenticated Page	Data Memory, W/C Counters of Memory Page and Secret, Secret, 64-bit ROM Registration Number, 160 bits of Scratchpad, Flags, PRNG Counter
Compute SHA	Several of the following Items, depending on selected Sub-Function: Data Memory, W/C Counter of Memory Page, Secret, 64-bit ROM Registration Number, Scratchpad, Flags, PRNG Counter

64 位光刻 ROM 图 3



1-Wire CRC 发生器 图 4



存储器映像

如框图所示，DS1963S 有 4 个存储区：数据存储器，密钥存储器，计数器存储器和暂存器。这些存储器区域被组织为 32 字节页。详见图 5 所示。当写数据或密钥时，暂存器被作为缓冲器使用。0 至 15 页可自由读/写。它们总计包含 4096 位的 NV SRAM。页 16 和 17 含有用户只可写入的八个 64 位密钥。密钥只能被 SHA 引擎读取，后者用它来计算信息鉴定码。16 个 32 位写循环计数器计算写入第 8 至 15 存储器页和 8 个密钥的次数。这些计数器位于页 19 和 20，可自由读取。第 21 页包括一个计数器，每次启动 SHA 引擎时都会递增。该计数器为产生伪随机数据提供种子，并因此而被称为 PRNG 计数器。由于 SHA 引擎所需的功耗要比复制整个暂存器到某存储区的功耗高出约 20 倍，PRNG 计数器的内容可用做器件剩余电量的指示。第 18 页是 32 字节暂存器的物理地址。

地址寄存器和传送状态

DS1963S 使用了 3 个地址寄存器：TA1，TA2 和 E/S（图 6）。寄存器 TA1 和 TA2 用来存放读写数据的目标地址。寄存器 E/S 是一个只读的字节计数器和传送状态寄存器，用来检验与写命令相关的数据的完整性。E/S 寄存器的低 5 位指示最后写入暂存器、以后将复制到主存储器的数据字节的地址。这个地址称为终止位置。E/S 寄存器的第 5 位称为 PF 或“半字节标志（partial byte flag）”，当主机写入的数据位数不是 8 的整数倍时被置为逻辑 1。位 6 无任何功能，读取时总是 0。需要注意的是，目标地址的低 5 位同时也决定了暂存器内部开始存放数据的起始地址。这个地址被称为字节偏移。例如，如果一条 Write（写）命令的目标地址（TA1）是 3Ch，那么暂存器将从字节偏移量 1Ch 处开始存放输入数据，并且 4 个字节后将会被充满，终止位置变为 1Fh。在执行一条 Write 命令后，主机可以利用终止位置和半字节标志来检验数据的完整性。E/S 寄存器的最高位 AA 或 Authorization Accepted（授权认可）用以指示暂存器中保存的数据已被复制到了目标存储器地址。写数据到暂存器将清除该标志。

DS1963S 存储器映像 图 5

允许读/写访问的数据存储器

4k 位 NV RAM

页号	地址范围	密钥号	计数器号	计数器递增条件
0	0000h 至 001Fh	0	0	无
1	0020h 至 003Fh	1	1	无
2	0040h 至 005Fh	2	2	无
3	0060h 至 007Fh	3	3	无
4	0080h 至 009Fh	4	4	无
5	00A0h 至 00BFh	5	5	无
6	00C0h 至 00DFh	6	6	无
7	00E0h 至 00FFh	7	7	无
8	0100h 至 011Fh	0	0	写循环
9	0120h 至 013Fh	1	1	写循环
10	0140h 至 015Fh	2	2	写循环
11	0160h 至 017Fh	3	3	写循环
12	0180h 至 019Fh	4	4	写循环
13	01A0h 至 01BFh	5	5	写循环
14	01C0h 至 01DFh	6	6	写循环
15	01E0h 至 01FFh	7	7	写循环

只允许用户写入的密钥存储器

页号	地址范围	说明
16	0200h 至 0207h	密钥 0
	0208h 至 020Fh	密钥 1
	0210h 至 0217h	密钥 2
	0218h 至 021Fh	密钥 3
17	0220h 至 0227h	密钥 4
	0228h 至 022Fh	密钥 5
	0230h 至 0237h	密钥 6
	0238h 至 023Fh	密钥 7

DS1963S 存储器映像（续） 图 5

只允许用户读取的密钥存储器

页号	地址范围	说明
19	0260h 至 0263h	计数器 0（页 8 的写循环）
	0264h 至 0267h	计数器 1（页 9 的写循环）
	0268h 至 026Bh	计数器 2（页 10 的写循环）
	026Ch 至 026Fh	计数器 3（页 11 的写循环）
	0270h 至 0273h	计数器 4（页 12 的写循环）
	0274h 至 0277h	计数器 5（页 13 的写循环）
	0278h 至 027Bh	计数器 6（页 14 的写循环）
	027Ch 至 027Fh	计数器 7（页 15 的写循环）
20	0280h 至 0283h	密钥 0 的写循环计数器
	0284h 至 0287h	密钥 1 的写循环计数器
	0288h 至 028Bh	密钥 2 的写循环计数器
	028Ch 至 028Fh	密钥 3 的写循环计数器
	0290h 至 0293h	密钥 4 的写循环计数器
	0294h 至 0297h	密钥 5 的写循环计数器
	0298h 至 029Bh	密钥 6 的写循环计数器
	029Ch 至 029Fh	密钥 7 的写循环计数器
21	02A0h 至 02A3h	PRNG 计数器

地址寄存器 图 6

目标地址（TA1）	T7	T6	T5	T4	T3	T2	T1	T0
目标地址（TA2）	T15	T14	T13	T12	T11	T10	T9	T8
截止地址和数据状态(E/S) (只读)	AA	0	PF	E4	E3	E2	E1	E0

写入及验证

为了向 DS1963S 写入数据，必须把暂存器用作中间存储器。首先，主控制器发 Write Scratchpad（写暂存器）命令并指定目的地址，然后将数据写入暂存器。在一定条件下（见“Write Scratchpad 命令”），主控在写暂存命令流程快结束时会收到一个反码的 CRC16，用于校验命令、地址和数据。知道了这个 CRC，主控制器将其与自己的计算结果相比较，就可以判断通信是否成功，以及是否继续 Copy Scratchpad 命令。如果主控制器未能收到 CRC16，则应该通过 Read Scratchpad（读暂存器）来验证数据的完整性。读暂存器时，在暂存器数据之前，DS1963S 会重新发回目的地址 TA1 和 TA2，以及 E/S 寄存器的内容。如果 PF 标志置位，说明数据未能正确送达暂存器。主控不必再继续读；它可尝试再次向暂存器写数据。类似地，如果 AA 标志置位，则说明器件未能认可 Write 命令。一切步骤正确的话，两个标志都清零，并且终止位置指向最后一个

写入暂存器的字节的地址。然后，主控制器可以继续读取和验证每个数据字节。验证数据后，主控制器就可以发 Copy Scratchpad 命令了。该命令之后必须紧随三个地址寄存器的内容：TA1，TA2 和 E/S。主控制器可以通过读暂存获得这些内容，或者也可以从目标地址和将要写入数据的数量中获得该信息。一旦 DS1963S 正确地收到这些字节，数据将被立即复制到从目标地址开始的规定位置。

存储器和 SHA 功能命令

DS1963S是专门为数据安全设计的器件，因而其操作与其他存储器iButton有所区别。DS1963S的数据存储器的读取方法和其他基于NV SRAM的存储器iButton一样，但是在读取页 16 和 17（用于存放密钥）、页 18（暂存器的物理地址）时，所得数据字节将为FFh，而非真实数据。DS1963S和其他常规存储器iButton所共有的一些功能由一个被称为HIDE的标志位控制。当这个HIDE标志被清零时，这些功能的使用和其他基于NV SRAM的器件相同。HIDE标志主要受控于（置位或清零）那些涉及到SHA引擎的操作。为防止暂存器数据偶然泄露，每次将DS1963S置于探头上，内部寄生供电的电路执行上电复位的同时，HIDE标志都会被自动置位。HIDE标志可通过Erase Scratchpad（擦除暂存器）命令清除，该命令同时擦除了留在暂存器内的全部数据。

“存储器和 SHA 功能流程”（图 7）描述了访问存储器和操作 SHA 引擎的必要协议。主机和 DS1963S 之间的通信可以常规速率（缺省，OD=0）或高速（OD=1）模式进行。如果没有明确设定为高速模式，DS1963S 总默认为常规速率。

Write Scratchpad 命令 [0Fh]

HIDE = 0，目标地址范围仅限于 0000h 至 01FFh

发出 Write Scratchpad 命令之后，主机必须首先提供两字节的目标地址，随后是要写入暂存器的数据。数据将由字节偏移（T4:T0）开始写入暂存器。终止位置（E4:E0）将是主机停止写入数据时的字节偏移。暂存器只接受完整的数据字节。如果最后一个数据字节不完整，它将被丢弃，半字节标志 PF 将被置位。

在执行 Write Scratchpad 命令时，DS1963S 内的 CRC 产生器（参见图 12）计算整个数据流的 CRC，始于命令代码，止于主机发送的最后一个数据字节。该 CRC 由一个 CRC16 多项式发生器产生，首先清除 CRC 产生器，然后移入 Write Scratchpad 命令码（0Fh），接着是由主机发出的目标地址 TA1、TA2 和所有数据字节。主机可随时结束 Write Scratchpad 命令。不过，如果终止位置为 11111b，主机就可以通过 16 个读时隙读到由 DS1963S 产生的 CRC。

HIDE = 1：目标地址范围仅限于 0200h 至 023Fh

该命令的功能仅限于选择密钥，选出的密钥即将被暂存器中的当前数据覆盖，这个数据通常是上一次运行 Compute First Secret（计算第一密钥）或 Compute Next Secret（计算下一密钥）命令后的结果。八个密钥的地址如图 5 所示。命令代码之后发送的地址可以指向密钥寄存器地址范围内的任何位置。紧随目标地址之后，主机可以象写暂存一样发送数据字节。一旦发送的数据字节填满由指定的目标地址开始的暂存器空间时，主机就可以通过 16 个读时隙读到由 DS1963S 产生的 CRC。数据字节被用于 CRC 的计算，但不会真正写入暂存器。

Read Scratchpad 命令[AAh]

HIDE = 0：

Read Scratchpad 命令用于验证目标地址、终止位置和暂存器中数据的完整性。发出命令代码后主机开始读入数据。前两个字节为目标地址。下一个字节是终止位置/数据状态字节（E/S），紧随其后的便是由字节偏移（T4:T0）开始的暂存器数据。主机可以一直读完暂存器，随后，便可收到由 DS1963S 生成的反码 CRC。如果主机在读完 CRC 后继续读，则读出数据全为逻辑 1。

HIDE = 1：

该命令的功能仅限于读取目标地址和终止位置。在读取暂存器数据时，主机收到的将为逻辑 1，直到暂存器底部，此后主机将收到由 DS1963S 产生的 CRC。如果主机继续读，读出数据将全为逻辑 1。

Copy Scratchpad [55h]

HIDE = 0：目标地址范围仅限于 0000h 至 01FFh

Copy Scratchpad 命令用于将暂存器数据复制到某存储页中。发出命令之后，主机必须发送一个 3 字节的授权码型，这个数据应该通过紧邻此条命令之前的一个 Read Scratchpad 命令获得。这个 3 字节码型必须与三个地址寄存器（依次为 TA1，TA2，E/S）中的数据完全匹配。如果码型匹配，AA（授权接受）标志将置位，并开始复制。当正在复制数据时，主机只能读到逻辑 1。数据复制结束后，它将向主机发送 1、0 交错的码型，直到主机发出复位脉冲（reset pulse）为止。当正在进行复制时，任何复位操作都将被忽略。复制操作需花费大约 30µs 的时间。主机必须读取至少 8 位交错码型，否则器件可能无法正确响应随后的复位脉冲。

三个地址寄存器中的内容决定了将要被复制的数据。暂存器中从起始偏移到终止位置间的数据将被复制到由目标地址开始的内存中。通过这条命令，可将 1 至 32 个字节的数据复制到内存中的任意位置。只有运行 Write Scratchpad 命令时 AA 标志才会被清除。

HIDE = 1：目标地址范围仅限于 0200h 至 023Fh

如果目标地址和终止位置与某个密钥相匹配，功能的执行和上述常规流程相同。如果目标地址指向主存储区地址范围中的某个位置，但是 HIDE 标志置位（例如，当寄生供电电路经历了上电复位之后），将不会复制任何暂存器数据。为了复制一个已知的数据（“口令”）到密钥中，我们可以先将数据写入暂存器，然后置位 HIDE 标志，发出一条 Write Scratchpad 命令以便选定一个密钥，最后，发一条 Copy Scratchpad 命令。不过，这种操作会降低系统的安全性，因此不建议使用。

Read Memory [F0h]

Read Memory（读存储器）命令可用来读取存储页 0 至 15、位于页 19 和 20 的写循环计数器和页 21 前端的 PRNG 计数器中的内容。位于页 16 和 17 密钥存储区中的数据不可读出。在读取页 18 时，如果 HIDE 标志清零（HIDE=0），将读回暂存器中的数据，如果该标志置位（HIDE=1），将返回 FFh。命令发出后，主机还必须提供 2 字节的目标地址。这两个字节之后，主机便可读出自目标地址开始的数据，读操作可一直持续到 PRNG 计数器的底部乃至于超出。PRNG 计数器之后还有 12 个未定义的字节。如果主机继续读，结果将为逻辑 1。需要特别注意的是，目标地址寄存器将指向最后一个读取的字节。终止位置/数据状态字节不受影响。

DS1963S 提供的硬件手段能够保证写入存储单元的数据正确无误。为了保证在 1-Wire 环境下读取数据的可靠性，同时提高数据传输的速率，建议将数据按照存储器页的大小进行分组。然后，在每个分组内包含一个由主控制器计算的、针对每页数据的 16 位 CRC。这样，主控制器就不必多次重复地读取一页数据来检验数据的正确与否，从而保证了快速、无误地传输数据（推荐的文件结构参见应用笔记 114，有时也称之为 TMEX 格式）。

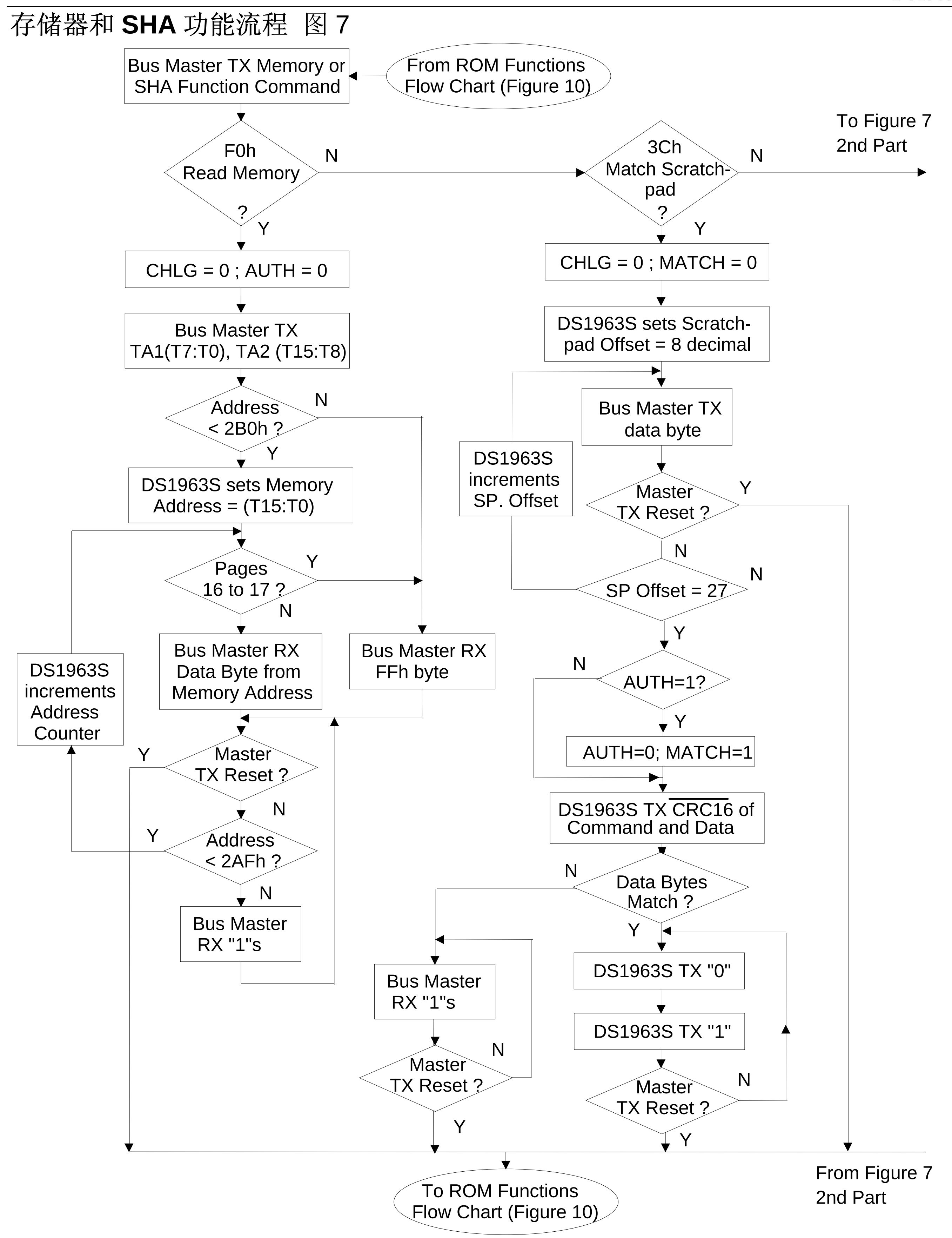
Erase Scratchpad [C3h]

该命令的目的是清零 HIDE 标志和擦除前次操作留在暂存器中的数据。发送命令码后，如 Write Scratchpad 命令那样，主机发送一个目标地址，但不发送数据。接下来整个暂存器将被自动添满 FFh 字节，而与目标地址无关。此过程用时约 32µs，其间主机将读到 1。此后主机会读到一个 0、1 交替的码型，表示命令执行完毕。主机必须读取至少 8 位交错码型，否则器件可能无法正确响应随后的复位脉冲。

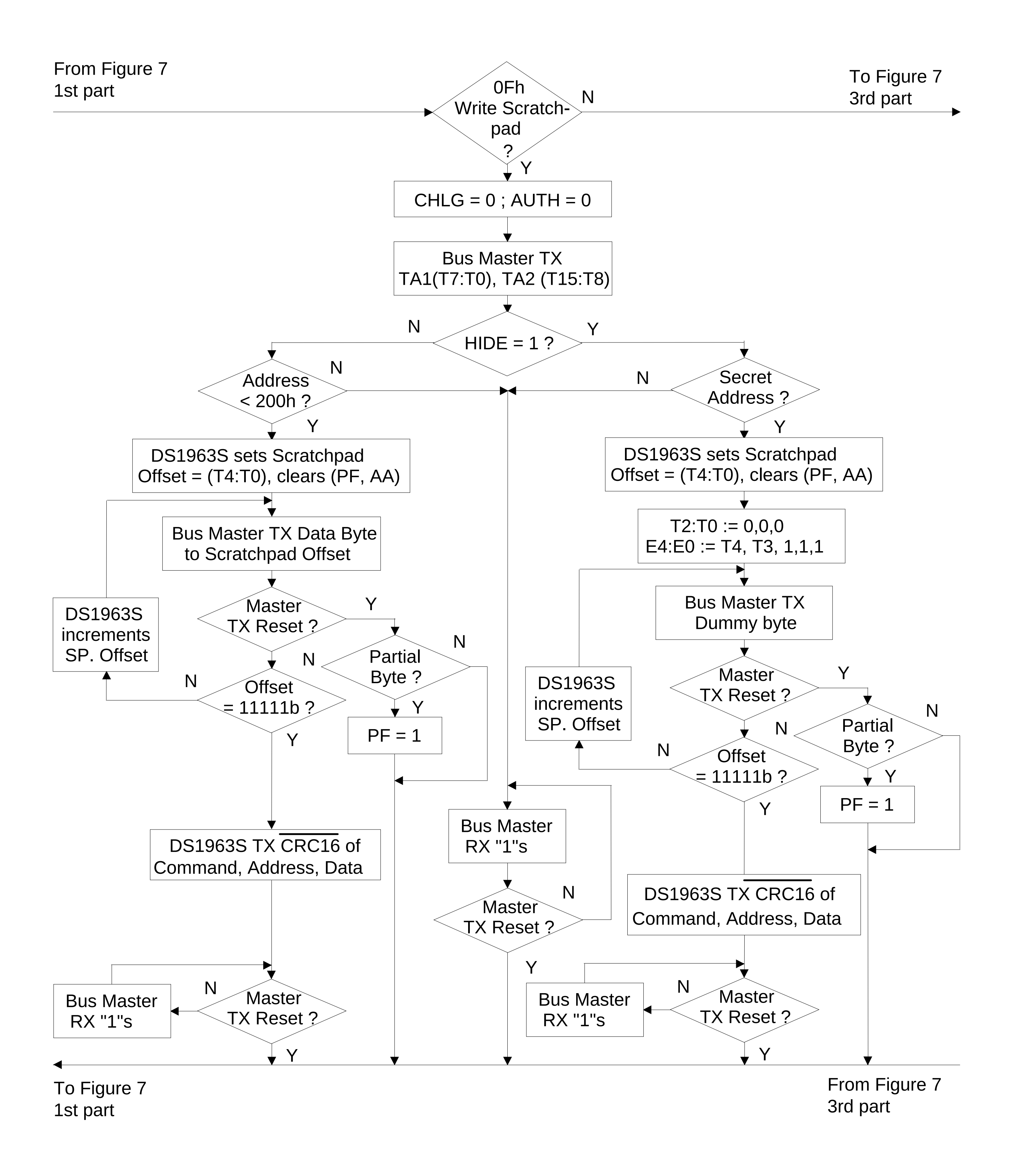
Match Scratchpad [3Ch]

由 DS1963S 计算出的 SHA-1 MAC 被写入暂存器中。有些操作中，例如 Authenticate Host（主机认证）和 Validate Data Page（数据页确认），执行运算的同时还会置位 HIDE 标志。通过 Match Scratchpad（匹配暂存器）命令可实现对于该数据有效性的检验，同时又不需要将其读出。每执行一次 SHA 运算后（关于算法的详细说明参见“SHA-1 算法”和“SHA-1 输出信息格式”章节），160 位的信息鉴定码被保存在暂存器偏移地址 8 至 27 中，通过该条命令，可以将它与主机自己的计算结果相比较。Match Scratchpad 命令发出后，主机开始逐字节发送数据，从第 8 字节开始到第 27 字节结束。如果所有字节匹配，主机就会读到一个 0、1 交替的码型。如果 AUTH 标志置位，MATCH 标志也被置位。如果匹配不成功，主机将读到全 1。收到反码的 CRC16 后主机必须读取至少 8 位交错码型，否则器件可能无法正确响应随后的复位脉冲。

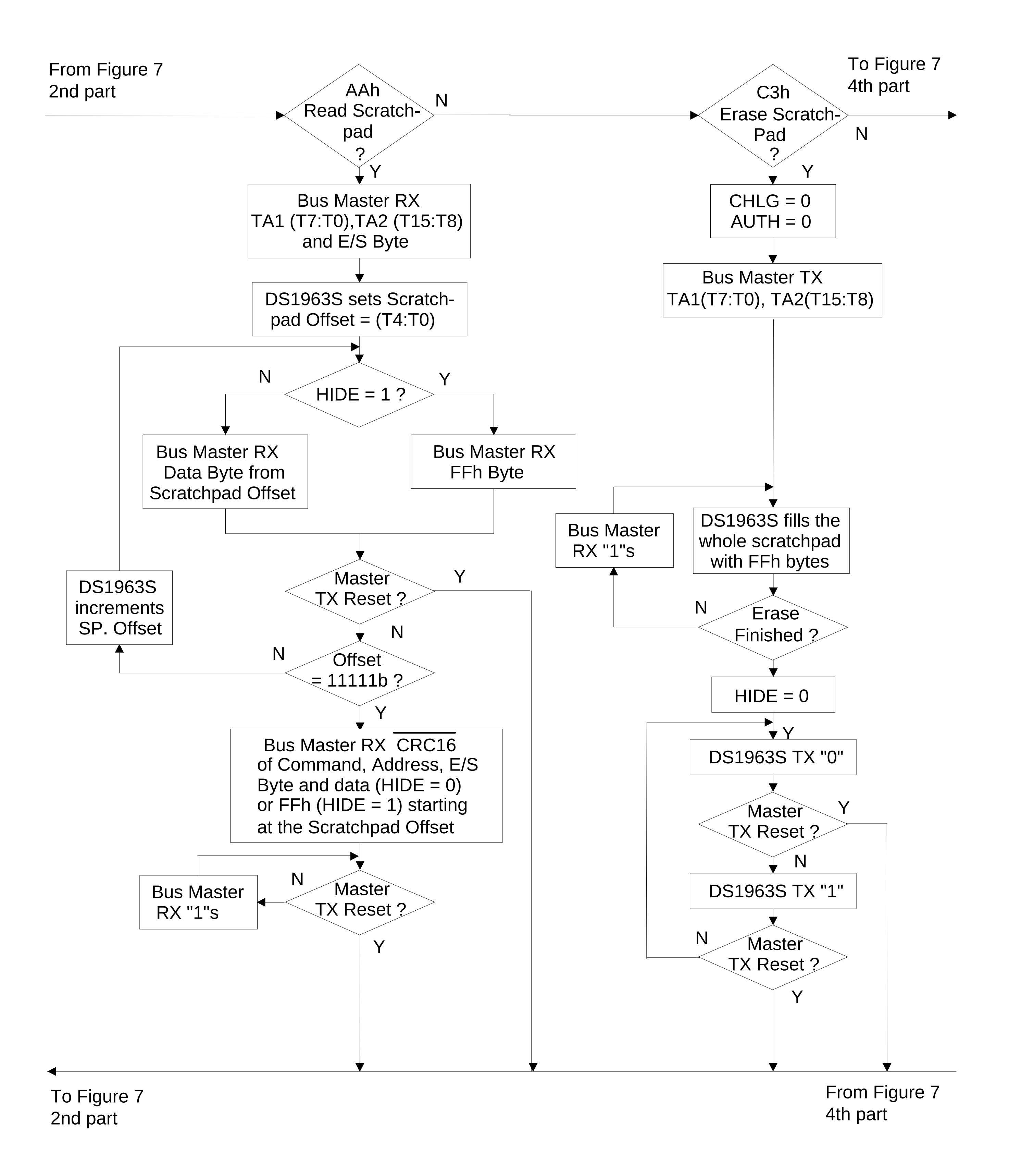
存储器和 **SHA** 功能流程 图 7



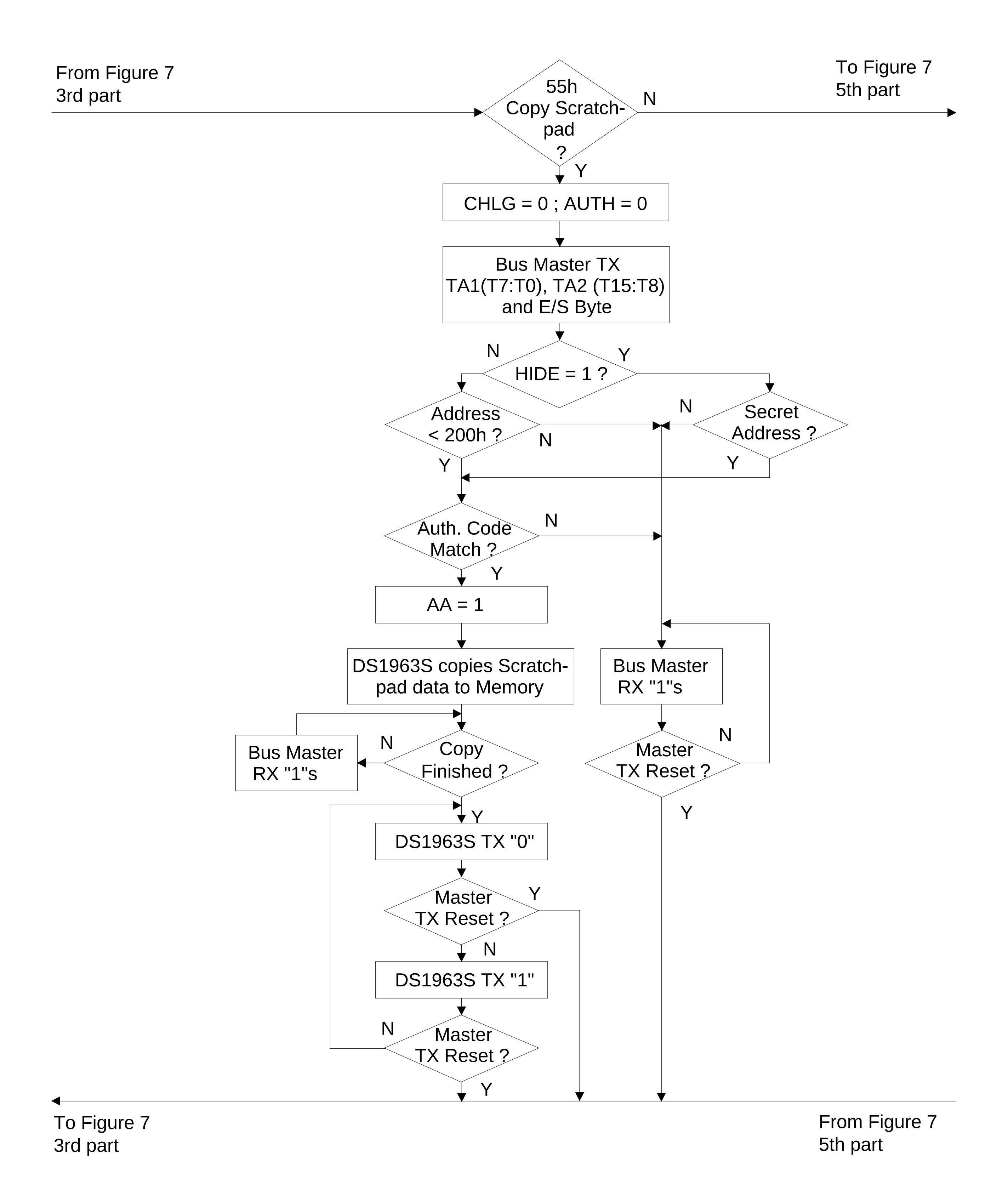
存储器和 **SHA** 功能流程（续） 图 7



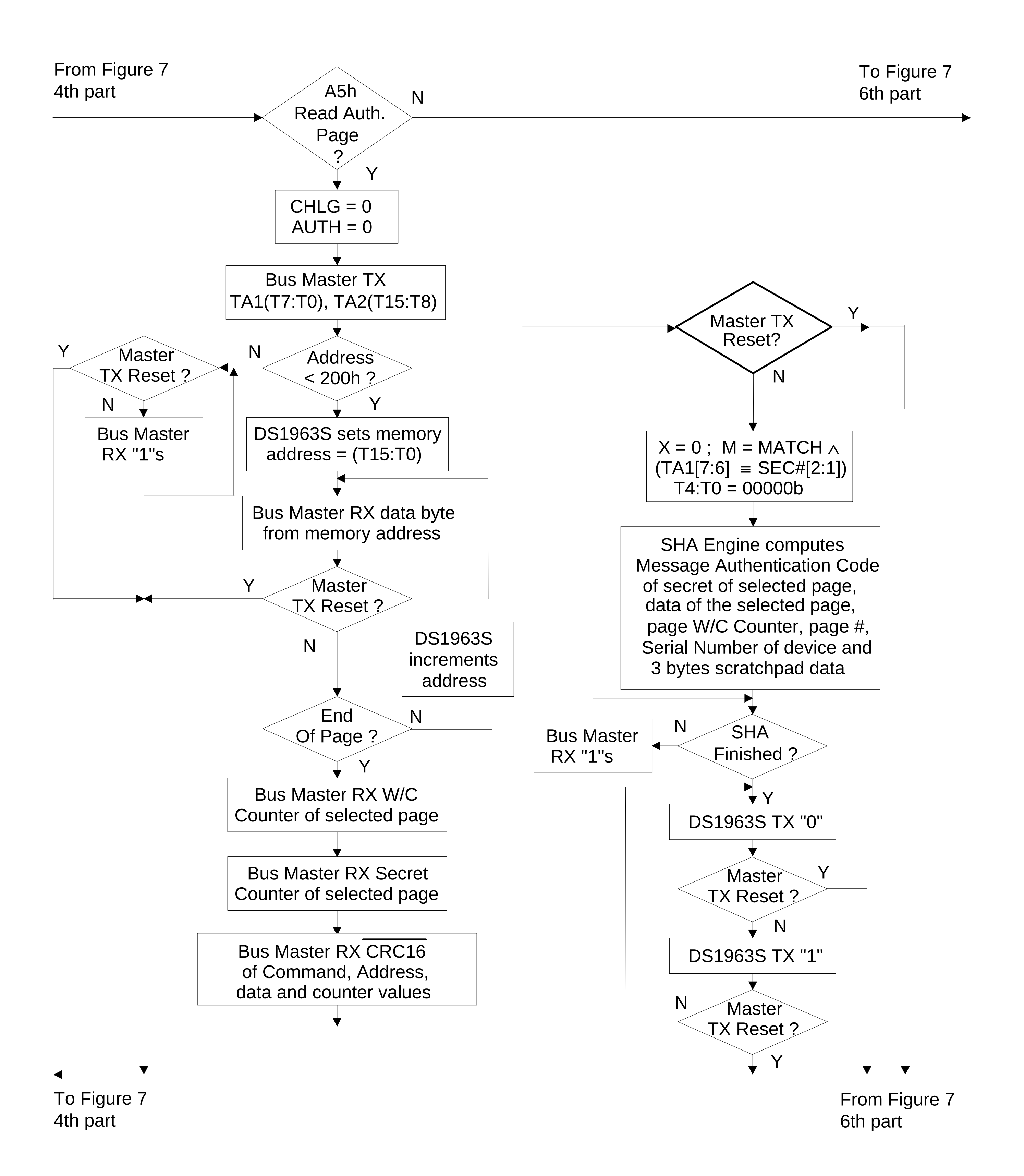
存储器和 **SHA** 功能流程（续） 图 7



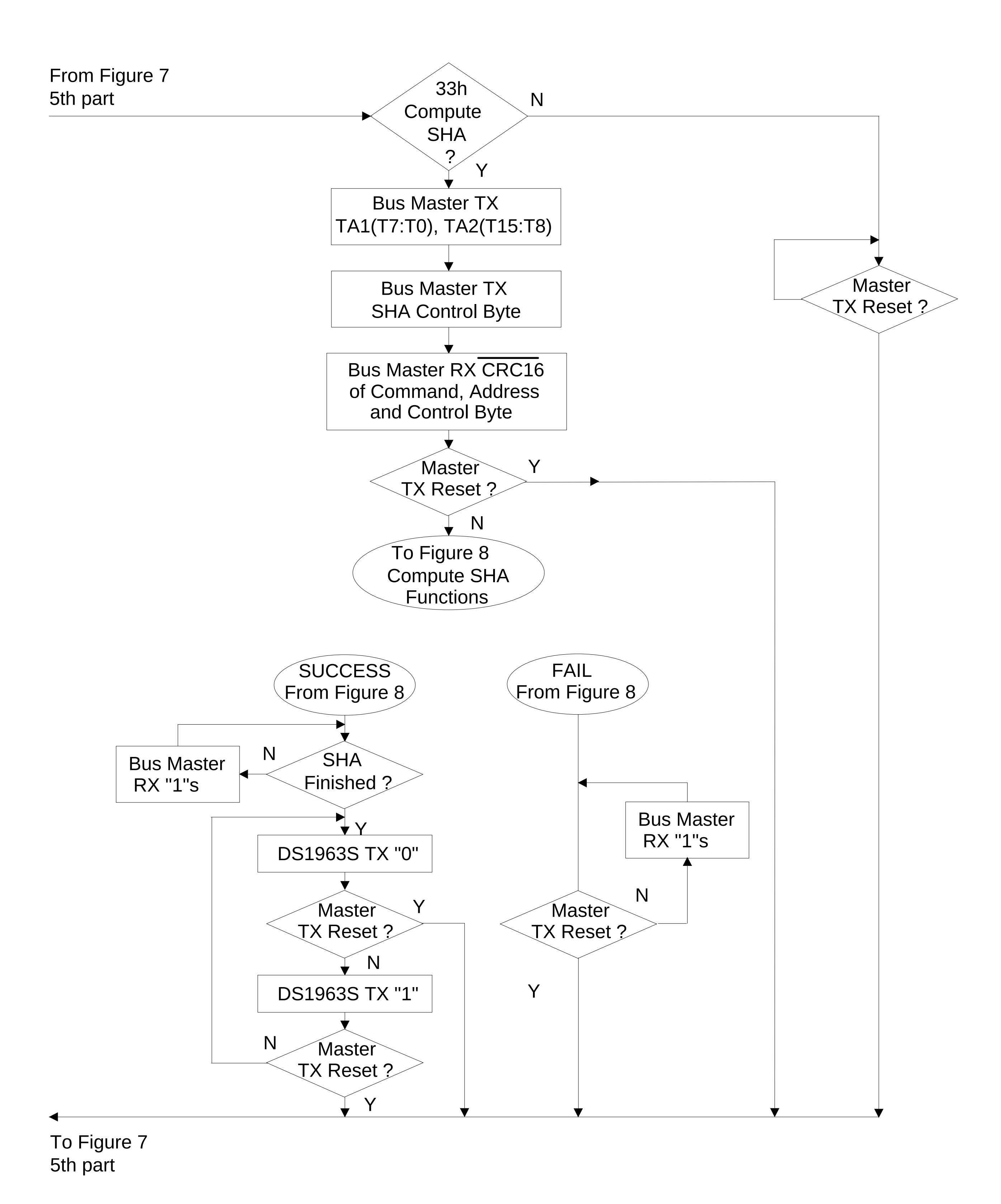
存储器和 **SHA** 功能流程（续） 图 7



存储器和 **SHA** 功能流程（续） 图 7



存储器和 **SHA** 功能流程（续） 图 7



Read Authenticated Page [A5h]

本命令仅适用于第 0 至第 15 页，用来读出全部或部分存储页，同时计算出一个 SHA-1 信息鉴定码。当主机发出命令码并指定了一个有效的目标地址后，它将依次收到从目标地址开始直到指定数据页结束的所有数据，该页写循环计数器的值，该页相关密钥的写循环计数器的值，以及针对命令码、目标地址、数据和计数器值的反码 CRC。读完 CRC 后，SHA 引擎立即开始以选定页的相关密钥、选定页的所有 32 字节数据、该页的写循环计数器、页号、器件的 ROM 注册码以及一个 3 字节的“质询”（取自暂存器的第 20 至 22 字节）等信息为输入计算信息鉴定码。SHA 计算结果被保存在暂存器中第 8 至 27 字节以备主机读取。当正在进行 SHA 计算时，主机将读到全 1。计算结束后，主机将交替读到 0 和 1。主机必须读取至少 8 位交错码型，否则器件可能无法正确响应随后的复位脉冲。接下来，主机通常是利用读到的页内数据等其他信息，自己计算一个信息鉴定码（参见 Compute SHA（计算 SHA）命令，“Validate Data Page”功能），并将它与暂存器中的数据相比较，根据比较结果判断 DS1963S 是否持有正确的指定数据页相关密钥。

Compute SHA [33h]

Compute SHA 命令给外部系统提供了六种利用 SHA 引擎以不同方法产生信息鉴定码的功能。操作 SHA 引擎的第七种方法是命令 Read Authenticated Page（读认证页），这已在前面一小节有所提及。有关各种 SHA 计算的全部细节在本节给出。表 1 列出了这些功能的概况。

SHA 功能概况 表 1

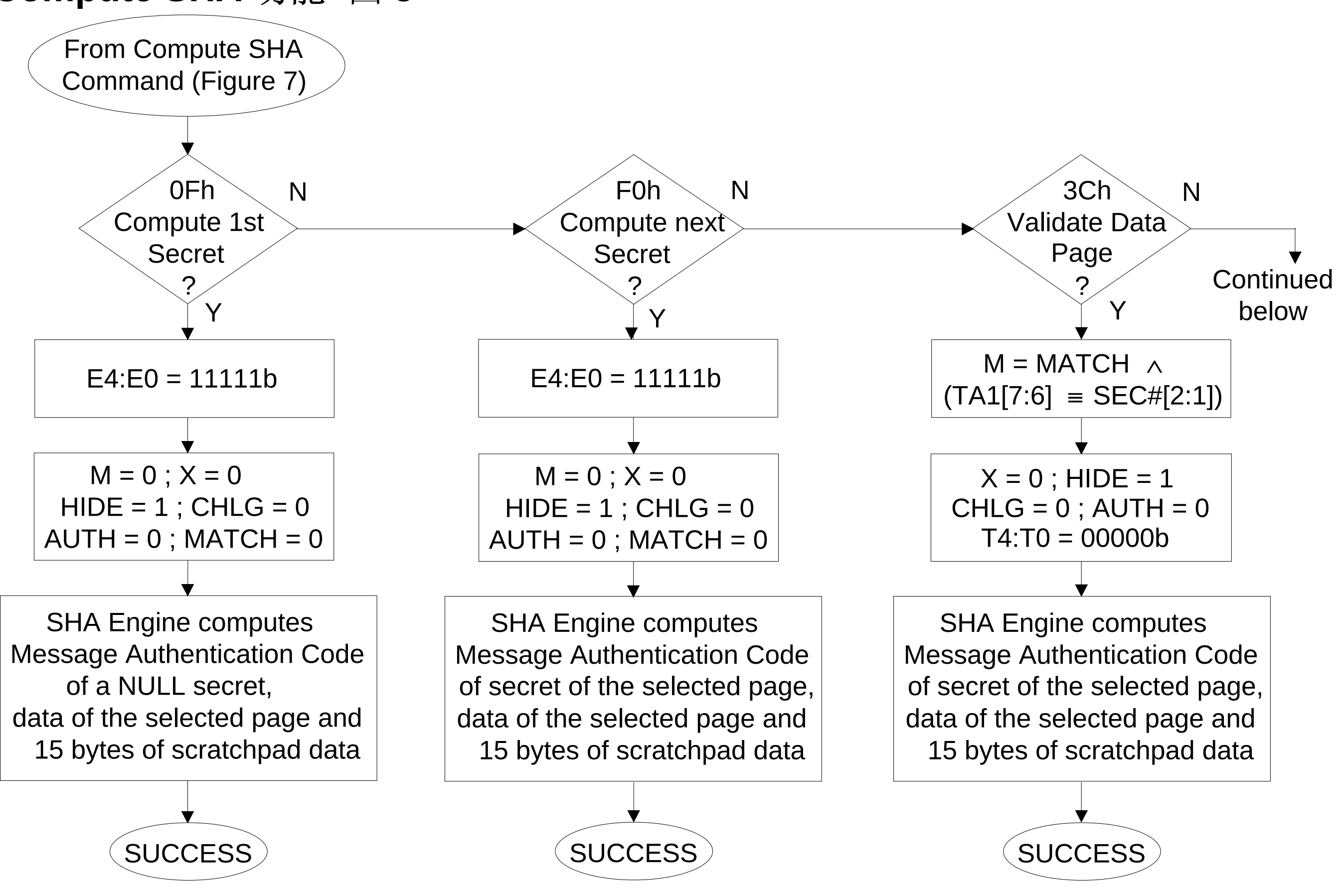
命令或功能名	漫游式钮扣	协处理器钮扣	适用范围
Read Authenticated Page	是	—	第 0 至 15 页
Validate Data Page 功能	—	是	第 0 至 15 页
Sign Data Page（标记数据页）功能	—	是	第 0 和第 8 页
Compute Challenge（计算质询）功能	是	—	除第 0 和第 8 页外
Authenticate Host 功能	是	—	除第 0 和第 8 页外
Compute First Secret 功能	是	是	第 0 至 15 页
Compute Next Secret 功能	是	是	第 0 至 15 页

在一个系统中，DS1963S 可以有两种使用方法：a) 由持有人携带的移动数据载体，以及 b) 作为主计算机或“总线主控”的一个协处理器和数据保险柜。无论何种应用，都要求在 DS1963S 中安装一个密钥。安装密钥需要一步或多步操作，这些用于安装密钥的功能称为 Compute First Secret 和 Compute Next Secret。作为协处理器使用的 DS1963S 需要完成两个功能：a) 确认一个漫游器件是否从属于本系统（也就是说，验证它是否知道密钥），以及 b) 生成或检验签名，以防数据被篡改。这些功能通过命令 Validate Data Page 和 Sign Data Page 实现。

漫游器件的主要 SHA 功能是 Read Authenticated Page，用来为协处理器提供执行 Validate Data Page 功能所需的数据和信息鉴定码。其余两个由漫游器件执行的 SHA 功能是 Compute Challenge 和 Authenticate Host。这些功能在有些应用（例如自动售货机）中不会用到。但是，这些功能在用户及主机的鉴别中必不可少，它们可以置位漫游器件的 MATCH 标志。由于在 Read Authenticated Page、Validate Data Page 和 Sign Data Page 等 SHA 运算过程中用到了 MATCH 标志，因而计算出的信息鉴定码有赖于并且揭示出主机鉴别是否成功。如果执行用户及主机鉴别，就不可将 DS1963S 作为协处理器使用，因为置位 MATCH 标志需要数个步骤。

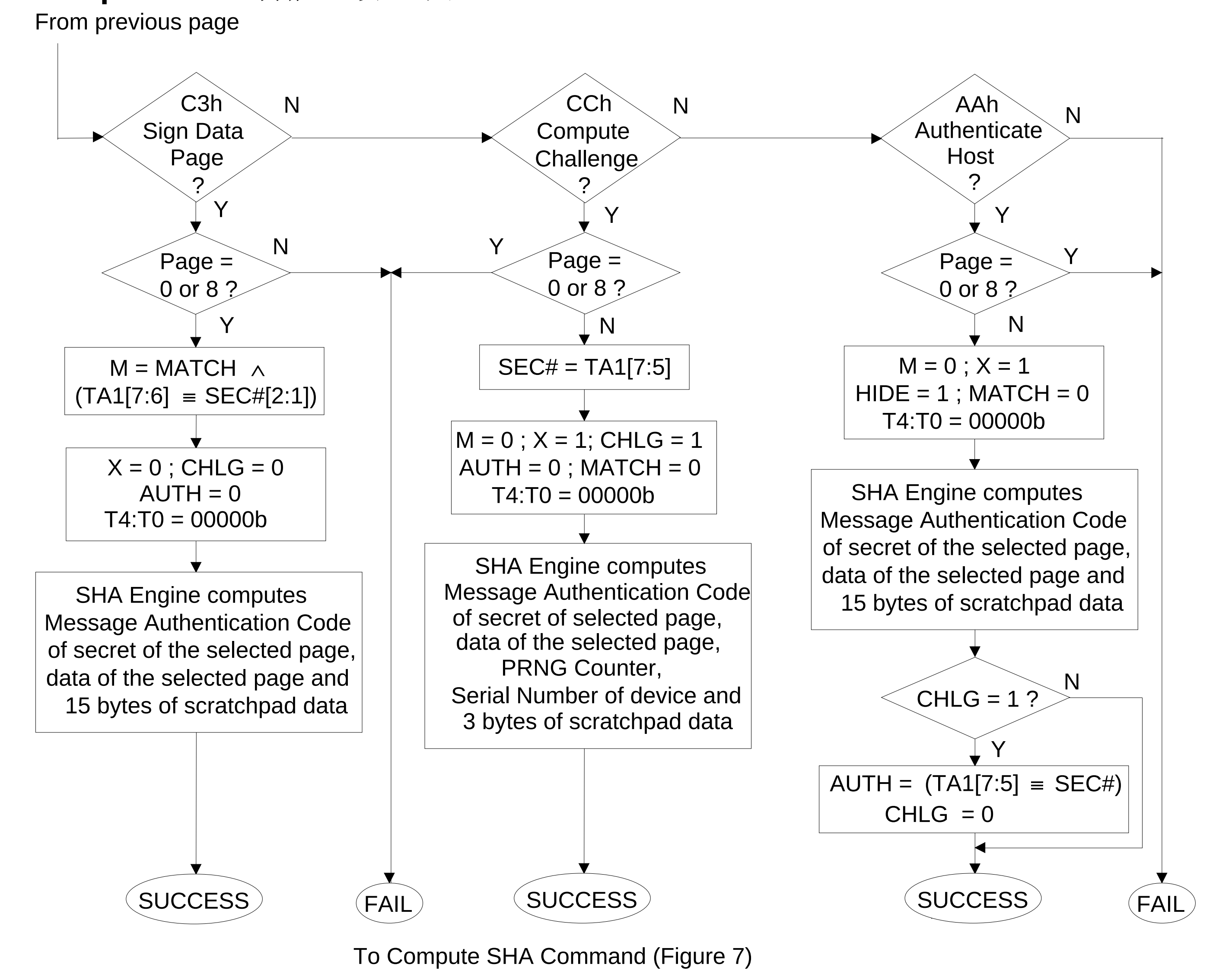
发送命令代码后，总线主控发送一个指向某一页内任意位置的目标地址，从而选定该存储页及其密钥。接下来主机发送 SHA 控制字节，它是六种 SHA 功能之一的代码。随后主机会收到一个用于校验命令代码、地址和控制字节的 CRC。一旦收到 CRC、并且确认控制字节和地址有效，将立即启动 SHA 引擎，按照图 8 所示计算一个消息认证代码。SHA 正在运算时主机将读到全 1。计算结束后读到的码型变为交替的 0 和 1。主机必须读取至少 8 位交错码型，否则器件可能无法正确响应随后的复位脉冲。如果控制码或地址无效，主机将始终读到全 1，直到发出复位脉冲。不同数据段在 SHA 引擎输入缓冲器中的准确位置如表 2 所示。

Compute SHA 功能 图 8



Read Authenticated Page 和 Compute Challenge 命令允许主机通过暂存器第 20 至 22 字节输入一个 3 字节“质询”。所有其它数据分别取自选定的存储页、相关密钥、循环计数器、ROM 注册号和标志位。在执行 Compute First Secret 和 Compute Next Secret 功能时，应在启动 SHA 运算前向暂存器的第 8 至 22 字节填入部分密钥数据。作为协处理器使用的器件在执行 Validate Data Page 或 Sign Data Page 命令时，须在暂存器第 8 至 11 字节存入（递增）与选定的漫游器件存储页相关的循环计数器的值，并且在第 13 至 19 字节存入 ROM 注册号（不包括 CRC），在第 12 字节存入页号。漫游器件在执行 Authenticate Host 命令前应首先执行 Compute Challenge 功能，以便在暂存器中填入伪随机数。

Compute SHA 功能（续） 图 8



Compute Challenge 功能将 TA1 的高三位保存在一个称为 SEC#的锁存器中，在接下来的 Authenticate Host 功能中会用到它。只有当 Authenticate Host 和 Compute Challenge 功能调用同一存储页（相同密钥）时 AUTH 标志才会置位。这样可以防止利用其它页的密钥（可能属于其他不同的应用或服务提供商）将 AUTH 标志置位。

当确定 M 控制位时 SEC#的高两位也被用于 Validate Data Page、Sign Data Page 和 Read Authenticated Page 功能，这只影响那些用到主机/用户鉴别的应用。只有当 MATCH 标志置位，并且目标存储页相邻于用于鉴别的页时，M 控制位才置位。这样就将一对密钥（0 和 1，2 和 3，4 和 5，6 和 7）及其相关存储页分配给了一个服务提供商。

SHA-1 输入信息格式　表 2

Read Authenticated Page 命令，Compute Challenge 功能

M0[31:24] = (SS+0)	M0[23:16] = (SS+1)	M0[15:8] = (SS+2)	M0[7:0] = (SS+3)
M1[31:24] = (PP+0)	M1[23:16] = (PP+1)	M1[15:8] = (PP+2)	M1[7:0] = (PP+3)
M2[31:24] = (PP+4)	M2[23:16] = (PP+5)	M2[15:8] = (PP+6)	M2[7:0] = (PP+7)
M3[31:24] = (PP+8)	M3[23:16] = (PP+9)	M3[15:8] = (PP+10)	M3[7:0] = (PP+11)
M4[31:24] = (PP+12)	M4[23:16] = (PP+13)	M4[15:8] = (PP+14)	M4[7:0] = (PP+15)
M5[31:24] = (PP+16)	M5[23:16] = (PP+17)	M5[15:8] = (PP+18)	M5[7:0] = (PP+19)
M6[31:24] = (PP+20)	M6[23:16] = (PP+21)	M6[15:8] = (PP+22)	M6[7:0] = (PP+23)
M7[31:24] = (PP+24)	M7[23:16] = (PP+25)	M7[15:8] = (PP+26)	M7[7:0] = (PP+27)
M8[31:24] = (PP+28)	M8[23:16] = (PP+29)	M8[15:8] = (PP+30)	M8[7:0] = (PP+31)
M9[31:24] = (CC+0)	M9[23:16] = (CC+1)	M9[15:8] = (CC+2)	M9[7:0] = (CC+3)
M10[31:24] = MP	M10[23:16] = FAMC	M10[15:8] = SN0	M10[7:0] = SN1
M11[31:24] = SN2	M11[23:16] = SN3	M11[15:8] = SN4	M11[7:0] = SN5
M12[31:24] = (SS+4)	M12[23:16] = (SS+5)	M12[15:8] = (SS+6)	M12[7:0] = (SS+7)
M13[31:24] = (SP+20)	M13[23:16] = (SP+21)	M13[15:8] = (SP+22)	M13[7:0] = 80h
M14[31:24] = 00h	M14[23:16] = 00h	M14[15:8] = 00h	M14[7:0] = 00h
M15[31:24] = 00h	M15[23:16] = 00h	M15[15:8] = 01h	M15[7:0] = B8h

符号

Mt	**SHA** 引擎的输入缓冲器 0 ≤ t ≤ 15; 32 位字
SS	密钥起始地址 见图 5，存储器映像，存储页 16 和 17
CC	写循环计数器起始地址 *Read Authenticated Page 命令：*选定存储页的写循环计数器，见图 5，存储器映像，存储页 19；计数器低字节保存在低地址 *Compute Challenge：*PRNG 计数器；见图 5，存储器映像，存储页 21；计数器低字节保存在低地址
PP	存储页的起始地址 见图 5，存储器映像，存储页 0 和 15
FAMC	家族码 **= 18h**
MP	MP[7] = 控制位 M，见图 7，Read Authenticated Page，和图 8 MP[6] = 控制位 X，见图 7，Read Authenticated Page，和图 8 MP[5:4] = 00b MP[3:0] = T8:T5（等同于 16 进制页号）
SNx	器件的 **ROM** 序列号 SN0 = 最低字节，SN5 = 最高字节 CRC 没有使用
(SP+n)	暂存器第 **n** 字节 n 为 10 进制数

SHA-1 输入信息格式（续） 表 2

Validate Data Page, Sign Data Page, Authenticate Host, Compute First Secret, Compute Next Secret

M0[31:24] = (SS+0)	M0[23:16] = (SS+1)	M0[15:8] = (SS+2)	M0[7:0] = (SS+3)
M1[31:24] = (PP+0)	M1[23:16] = (PP+1)	M1[15:8] = (PP+2)	M1[7:0] = (PP+3)
M2[31:24] = (PP+4)	M2[23:16] = (PP+5)	M2[15:8] = (PP+6)	M2[7:0] = (PP+7)
M3[31:24] = (PP+8)	M3[23:16] = (PP+9)	M3[15:8] = (PP+10)	M3[7:0] = (PP+11)
M4[31:24] = (PP+12)	M4[23:16] = (PP+13)	M4[15:8] = (PP+14)	M4[7:0] = (PP+15)
M5[31:24] = (PP+16)	M5[23:16] = (PP+17)	M5[15:8] = (PP+18)	M5[7:0] = (PP+19)
M6[31:24] = (PP+20)	M6[23:16] = (PP+21)	M6[15:8] = (PP+22)	M6[7:0] = (PP+23)
M7[31:24] = (PP+24)	M7[23:16] = (PP+25)	M7[15:8] = (PP+26)	M7[7:0] = (PP+27)
M8[31:24] = (PP+28)	M8[23:16] = (PP+29)	M8[15:8] = (PP+30)	M8[7:0] = (PP+31)
M9[31:24] = (SP+8)	M9[23:16] = (SP+9)	M9[15:8] = (SP+10)	M9[7:0] = (SP+11)
M10[31:24] = MPX	M10[23:16] = (SP+13)	M10[15:8] = (SP+14)	M10[7:0] = (SP+15)
M11[31:24] = (SP+16)	M11[23:16] = (SP+17)	M11[15:8] = (SP+18)	M11[7:0] = (SP+19)
M12[31:24] = (SS+4)	M12[23:16] = (SS+5)	M12[15:8] = (SS+6)	M12[7:0] = (SS+7)
M13[31:24] = (SP+20)	M13[23:16] = (SP+21)	M13[15:8] = (SP+22)	M13[7:0] = 80h
M14[31:24] = 00h	M14[23:16] = 00h	M14[15:8] = 00h	M14[7:0] = 00h
M15[31:24] = 00h	M15[23:16] = 00h	M15[15:8] = 01h	M15[7:0] = B8h

符号

Mt	**SHA** 引擎的输入缓冲器 0 ≤ t ≤ 15; 32 位字
SS	密钥起始地址 见图 5，存储器映像，存储页 16 和 17 在 Compute First Secret 时密钥数据为全零。
PP	存储页的起始地址 见图 5，存储器映像，存储页 0 至 15
MPX	MPX[7] = 控制位 M，见图 8 MPX[6] = 控制位 X，见图 8 MPX[5:0] = (SP+12)[5:0]
(SP+n)	暂存器第 **n** 字节 n 为 10 进制数

SHA 功能和存储器功能中用到了几个标志，它们会影响到本功能以及后续操作的结果。这些标志包括 HIDE、CHLG、AUTH 和 MATCH。表 3 归纳了这些标志的工作情况。唯一不影响任何标志的命令是 Read Scratchpad。需要注意的是，器件中采用寄生供电的 1-Wire 前端电路在上电复位时也会影响标志。“Return to Probe（返回探测器）”状态一般出现在某个 DS1963S 器件和主机/总线主控的读/写头发生接触或断续接触时。意义最为明显的就是 HIDE 标志，它置位后可阻止用户读取暂存器中的数据；不过，仍可读出目标地址和 E/S 字节寄存器的内容。HIDE 标志也影响 Write Scratchpad 和 Copy Scratchpad 命令。其他三个标志仅在某些特殊情况下使用，多数时间为零。CHLG 和 AUTH 标志在主机/用户鉴别过程中配对使用，用来保证命令按照特定顺序执行。如果顺序正确，并且在后续的 Match Scratchpad 命令中数据匹配成功，则 MATCH 标志置位。在接下来的操作中，MATCH 标志会影响 Validate Data Page，Sign Data Page 或 Read Authenticated Page 功能。

器件标志总结 表 3

命令、功能或状态	HIDE	CHLG	AUTH	MATCH
Return to Probe 状态	置位	-----	-----	-----
Read Memory 命令	-----	清零	清零	-----
Match Scratchpad 命令	-----	清零	清零	注释 1
Write Scratchpad 命令	-----	清零	清零	-----
Read Scratchpad 命令	-----	-----	-----	-----
Erase Scratchpad 命令	清零	清零	清零	-----
Copy Scratchpad 命令	-----	清零	清零	-----
Read Authenticated Page 命令	-----	清零	清零	-----
Validate Data Page 功能	置位	清零	清零	-----
Sign Data Page 功能	-----	清零	清零	-----
Compute Challenge 功能	-----	置位	清零	清零
Authenticate Host 功能	置位	清零	注释 2	清零
Compute First Secret 功能	置位	清零	清零	清零
Compute Next Secret 功能	置位	清零	清零	清零

1) 如果数据匹配且在命令执行前 AUTH 标志已置位则标志置位；否则标志清零。置位 MATCH 标志需要连续、成功地运行 Compute Challenge、Authenticate Host 和 Match Scratchpad 命令。
2) 只有在执行命令前 CHLG 标志已置位时标志置位；否则清零。

SHA-1 算法

以下有关SHA算法的说明译自安全散列标准SHA-1 文档，参考该文档的第 2 页。该算法采用 16 个 32 位字M_t（$0 \le t \le 15$）作为输入数据，参见表 2，SHA-1 输入信息格式。SHA算法涉及到一个称为W_t（$0 \le t \le 79$）的 80 个 32 位字的序列，一个称为K_t（$0 \le t \le 79$）的 80 个 32 位字的序列，一个布尔函数f_t（B，C，D）（$0 \le t \le 79$），其中B，C和D为 32 位字，以及另外三个 32 位字，称为A，E和TMP。SHA算法用到的操作有不带进位的算术加（“+”），逻辑反或 1 的补码（“\”），异或（“⊕”），逻辑与（“∧”），逻辑或（“∨”），赋值（“:=”），以及 32 位字的循环移位。表达式“$S^n(X)$”表示将X向左循环移n位，X是一个 32 位字。

函数 f_t 定义如下：

$f_t(B,C,D) = (B \wedge C) \vee ((B\backslash) \wedge D)$ $(0 \le t \le 19)$

$B \oplus C \oplus D$ $(20 \le t \le 39)$

$(B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$ $(40 \le t \le 59)$

$B \oplus C \oplus D$ $(60 \le t \le 79)$

序列 W_t $(0 \le t \le 79)$定义如下：

$W_t := M_t$ $(0 \le t \le 15)$

$S^1(W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16})$ $(16 \le t \le 79)$

序列 K_t (0 ≤ t ≤ 79)定义如下：

K_t	:=	5A827999h	(0 ≤ t ≤ 19)
		6ED9EBA1h	(20 ≤ t ≤ 39)
		8F1BBCDCh	(40 ≤ t ≤ 59)
		CA62C1D6h	(60 ≤ t ≤ 79)

变量 A, B, C, D, E 初始化如下：

A	:=	67452301h
B	:=	EFCDAB89h
C	:=	98BADCFEh
D	:=	10325476h
E	:=	C3D2E1F0h

当 t 从 0 循环到 79，执行了下面的一系列计算后，160 位 MAC 是 A，B，C，D 和 E 的串联（不考虑任何进位）：

TMP	:=	$S^5(A) + f_t(B,C,D) + W_t + K_t + E$
E	:=	D
D	:=	C
C	:=	$S^{30}(B)$
B	:=	A
A	:=	TMP

根据所选的 SHA 功能，信息鉴定码以两种不同方式被装载到 DS1963S 的暂存器中。在 Compute First Secret 和 Compute Next Secret 功能中，MAC 中的 64 位被反复装载，以便将其复制到八个密钥中的任何一个。在所有其它的 SHA 功能中，全部的 160 位结果被装载到暂存器中。表 4 显示了数据在暂存器中的放置方法。

SHA-1 输出信息格式 表 4

部分码（仅对 Compute First Secret 和 Compute Next Secret）

(SP+0) := E[7:0]	(SP+1) := E[15:8]	(SP+2) := E[23:16]	(SP+3) := E[31:24]
(SP+4) := D[7:0]	(SP+5) := D[15:8]	(SP+6) := D[23:16]	(SP+7) := D[31:24]
(SP+8) := E[7:0]	(SP+9) := E[15:8]	(SP+10) := E[23:16]	(SP+11) := E[31:24]
(SP+12) := D[7:0]	(SP+13) := D[15:8]	(SP+14) := D[23:16]	(SP+15) := D[31:24]
(SP+16) := E[7:0]	(SP+17) := E[15:8]	(SP+18) := E[23:16]	(SP+19) := E[31:24]
(SP+20) := D[7:0]	(SP+21) := D[15:8]	(SP+22) := D[23:16]	(SP+23) := D[31:24]
(SP+24) := E[7:0]	(SP+25) := E[15:8]	(SP+26) := E[23:16]	(SP+27) := E[31:24]
(SP+28) := D[7:0]	(SP+29) := D[15:8]	(SP+30) := D[23:16]	(SP+31) := D[31:24]

全部 160 位码（所有其它 SHA 功能）

(SP+8) := E[7:0]	(SP+9) := E[15:8]	(SP+10) := E[23:16]	(SP+11) := E[31:24]
(SP+12) := D[7:0]	(SP+13) := D[15:8]	(SP+14) := D[23:16]	(SP+15) := D[31:24]
(SP+16) := C[7:0]	(SP+17) := C[15:8]	(SP+18) := C[23:16]	(SP+19) := C[31:24]
(SP+20) := B[7:0]	(SP+21) := B[15:8]	(SP+22) := B[23:16]	(SP+23) := B[31:24]
(SP+24) := A[7:0]	(SP+25) := A[15:8]	(SP+26) := A[23:16]	(SP+27) := A[31:24]

1-Wire 总线系统

1-Wire 单总线系统是用一根数据线连接单个主机和一台或多台从机设备的系统。任何情况下，DS1963S 都作为从机设备来使用。总线主机一般为一个微控制器或 PC。对于小型配置，1-Wire 通信信号可以在软件的控制下，利用单个口线产生。在多探头网络中，建议使用 DS2480B 1-Wire 线驱动器芯片或基于该芯片的串口适配器（DS9097U 系列）。这样可以简化硬件设计，降低主处理器为了达到实时操作的开销。

对单总线系统的论述分为以下三个部分：硬件结构、处理流程和 1-Wire信令（信号类型和定时）。1-Wire通信协议规定总线的收发按照特殊时隙下的总线状态进行，由主机发出的同步脉冲下降沿初始化。需要了解更多关于通讯协议详细描述，请参考*Book of DS19xx iButton Standards*第四章。

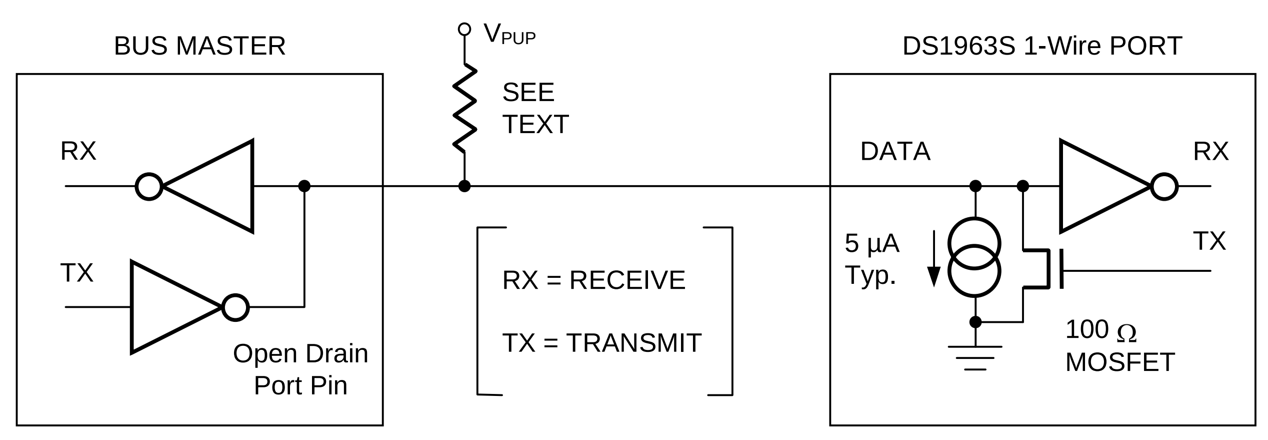
硬件配置

1-Wire 单总线系统中只定义了一根数据线，所以，保证在适当的时间驱动总线上的每个设备是非常重要的。为使上述操作易于实现，挂接在 1-Wire 总线上的每个装置必须都带有一个漏极开路或三态端口连接数据线。DS1963S 的 1-Wire 端口是漏极开路的，其内部等效电路如图 9 所示。

多点总线由连接了多个从机设备的 1-Wire总线组成。在常规速率下，1-Wire总线的最大速率为16.3kbps。在高速模式下，速率可达 142kbps。DS1963S不保证完全遵从iButton标准。它的最高数据速率在标准速度模式下为 15.4kbps，高速模式下为 125kbps。上拉电阻的值主要取决于网络的规模和负载条件。对于大部分应用来讲，2.2kΩ的最大阻值就足够了。

1-Wire 总线的空闲状态是高电平。如果由于某种原因需暂停通信，如果想稍候恢复通信的话，总线必须保持在空闲状态。如果不是这样，而总线又处于低电平状态超过 16µs（高速模式）或120µs（常规速度），那么总线上的一个或多个器件将被复位。对 DS1963S 而言，高速模式下总线拉低的时间不应长于 15.4µs，以保证 1-Wire 总线上没有从器件被复位。尽管它的兼容性有限，DS1963S 仍然可以和 DS2480B 1-Wire 驱动器和基于该驱动器的串口适配器正常通信。

硬件配置 图 9



处理流程

通过 1-Wire 端口访问 DS1963S 的协议如下：

- 初始化
- ROM 功能命令
- 存储器或 SHA 功能命令
- 会话/数据

初始化

1-Wire 总线上所有的传输操作均从初始化过程开始。初始化过程由总线主机发出的复位脉冲和从机发出的在线应答脉冲（presence pulse）组成。在线应答脉冲使主机检测到 DS1963S 挂接在总线上，并且已经准备就绪。详细内容请参阅“1-Wire 信令”一节。

ROM 功能命令

一旦主机检测到在线应答脉冲，就可以发出 DS1963S 支持的七条 ROM 功能命令之一。所有 ROM 功能命令的长度为八位。以下列出了这些命令的简要介绍（参考图 10 中的流程图）：

Read ROM [33h]

此条命令允许总线主机读取 DS1963S 的 8 位家族码、48 位唯一的序列号和 8 位 CRC 校验码。此命令适用于总线上只有一个从机的情况。如果总线上连接了多个从机设备，当同一时间每个从机设备都响应此条命令时，就必然要发生数据冲突（漏极开路输出将产生一个线与结果）。结果导致主机读取的家族码和 48 位序列号无效。

Match ROM [55h]

Match ROM 命令跟随 64 位 ROM 序列号，允许总线主机访问多从机总线系统中某个特定的 DS1963S。只有与 64 位 ROM 序列号完全匹配的 DS1963S 才会响应主机随后发出的存储器功能命令。所有与 64 位 ROM 序列号不匹配的从机将处于等待复位脉冲状态。这条命令既适用于单从机系统，也适用于多从机系统。

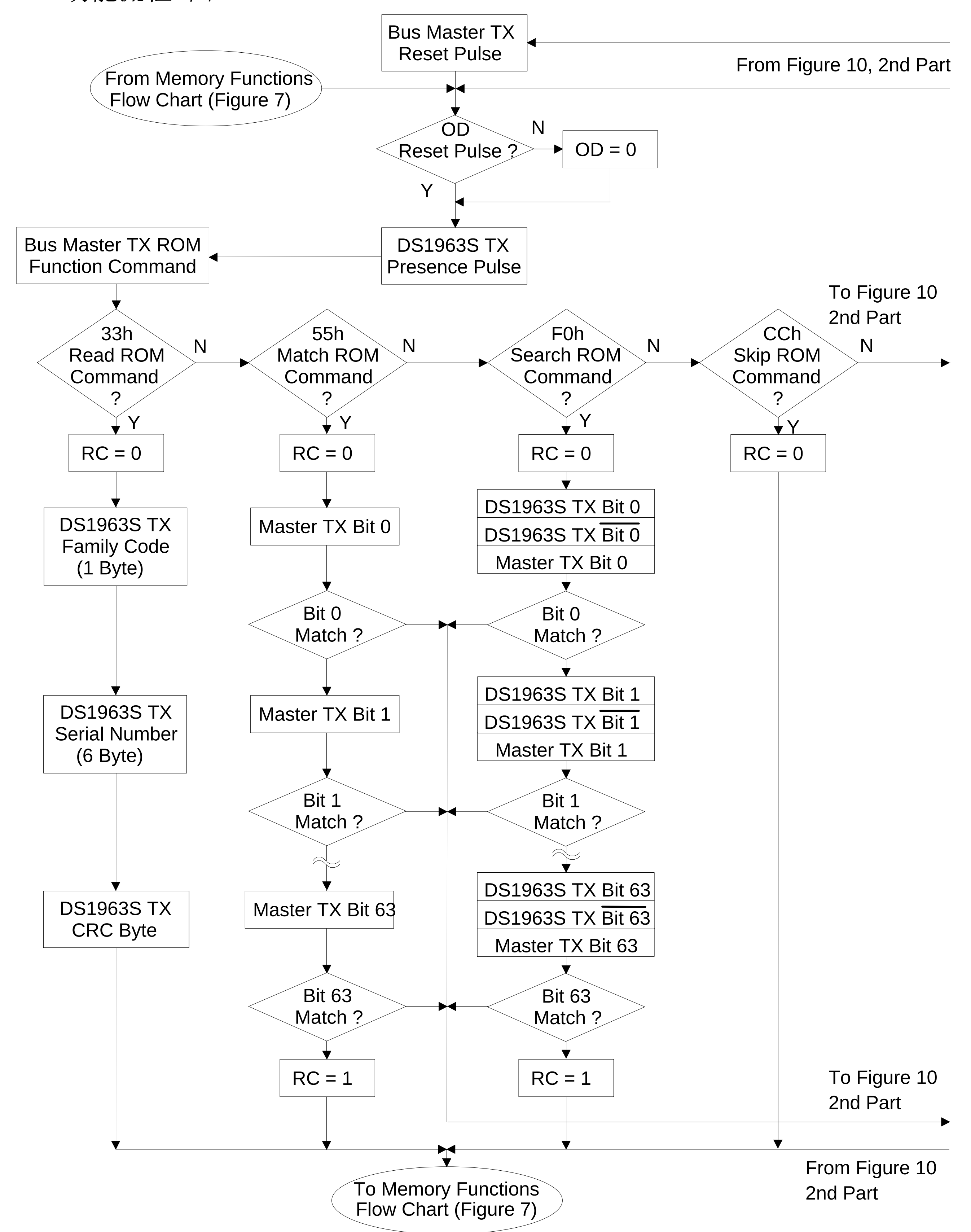
Search ROM [F0h]

系统初次上电时，总线主机可能并不知道 1-Wire总线上从机设备的数目和它们的 64 位ROM号，而search ROM命令能够使得总线主机通过排除法来检测出总线上所有从机设备的 64 位ROM号。search ROM过程其实只是 3 个简单步骤的重复：读一位、读此位的补码，然后写这一位的期望值，总线主机对ROM中的每一位数据都执行这简单的 3 步操作。在此操作全部审查通过之后，总线主机就能读出一台从机设备的 64 位ROM代码。其余从机设备的ROM代码可通过执行相同的操作检测出来。需要了解search ROM命令更全面的信息，请参考*Book of DS19xx iButton Standards*第五章，并且在此章中还包括一个实例。

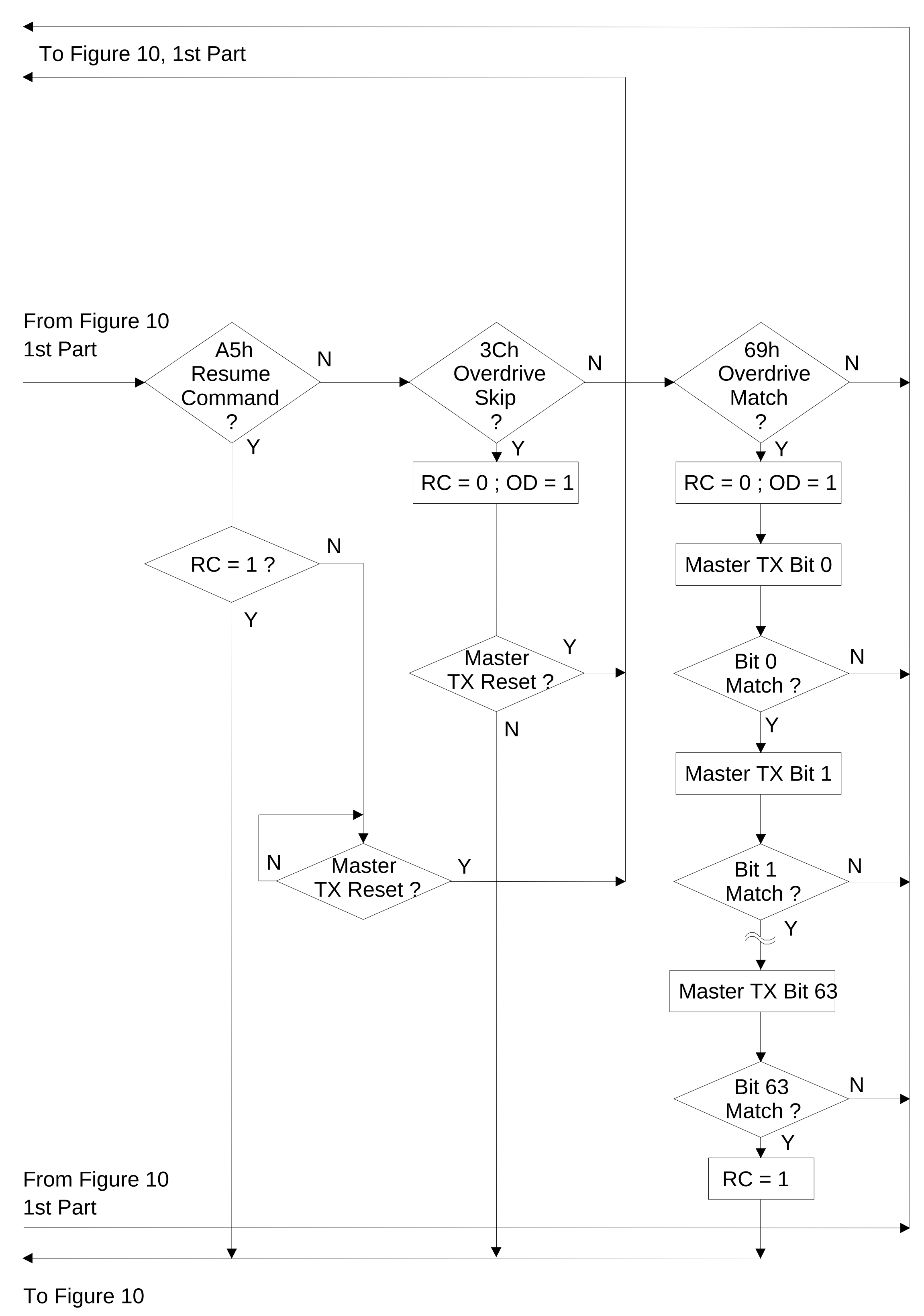
Skip ROM [CCh]

Skip ROM 命令在单从机总线系统中允许总线主机直接访问存储器和 SHA 功能，而无须提供 64 位 ROM 代码，节省时间。如果总线上挂接了不止一个从机设备，而且在 Skip ROM 命令后发出了一条读命令，总线上的从机设备就会同时传送数据，从而引起数据冲突（漏极开路输出将产生一个线与结果）。

ROM 功能流程 图 10


Bus Master TX Reset Pulse
From Figure 10, 2nd Part
From Memory Functions Flow Chart (Figure 7)
OD Reset Pulse ?
N
OD = 0
Y
Bus Master TX ROM Function Command
DS1963S TX Presence Pulse
To Figure 10 2nd Part
33h Read ROM Command ?
N
Y
55h Match ROM Command ?
N
Y
F0h Search ROM Command ?
N
Y
CCh Skip ROM Command ?
N
Y
RC = 0
RC = 0
RC = 0
RC = 0
DS1963S TX Family Code (1 Byte)
Master TX Bit 0
DS1963S TX Bit 0
DS1963S TX $\overline{\text{Bit 0}}$
Master TX Bit 0
Bit 0 Match ?
Bit 0 Match ?
DS1963S TX Serial Number (6 Byte)
Master TX Bit 1
DS1963S TX Bit 1
DS1963S TX $\overline{\text{Bit 1}}$
Master TX Bit 1
Bit 1 Match ?
Bit 1 Match ?
DS1963S TX CRC Byte
Master TX Bit 63
DS1963S TX Bit 63
DS1963S TX $\overline{\text{Bit 63}}$
Master TX Bit 63
Bit 63 Match ?
Bit 63 Match ?
RC = 1
RC = 1
To Figure 10 2nd Part
From Figure 10 2nd Part
To Memory Functions Flow Chart (Figure 7)

ROM 功能流程（续） 图 10



Overdrive Skip ROM [3Ch]

在单点总线上发出该命令的时候，总线主机不需要 64 位 ROM 码就可以执行存储器功能，从而节省了时间。不同于通常的 Skip ROM 命令，命令 Overdrive Skip ROM 将 DS1963S 设置成高速模式（OD = 1）。该命令代码后面的所有通信都发生在高速模式下，直到有一个最短持续 480μs 的复位脉冲把总线上的所有器件都复位到常规速率（OD = 1）。

在多点总线上发出该命令时，所有支持高速模式的器件都被置为高速模式。随后，为了寻址特定的高速模式器件，必须发出一个高速模式的复位脉冲，接着运用 Match ROM 或 Search ROM 命令。这将加速搜索过程。如果总线上有多于一个支持高速模式的从机，并且 Overdrive Skip ROM 命令后接着就是 Read 命令，那么由于多个从机同时发送，总线上就会发生数据冲突（多个开漏输出下拉将产生线与结果）。

Overdrive Match ROM [69h]

Overdrive Match ROM 命令后接以高速模式发送的 64 位 ROM 序列号，总线主控可以在多点总线上找到某个特定的 DS1963S，并将它设置成高速模式。只有 64 位 ROM 序列号精确匹配的 DS1963S 才会响应后续的存储器或 SHA 功能命令。那些通过前面的 Overdrive Skip 或成功执行 Overdrive Match 命令后已被置为高速模式的从机将继续保持高速模式。直到有一个最短持续时间 480μs 的复位脉冲发出后，所有高速模式的器件将返回常规速度。命令 Overdrive Match ROM 适用于总线上有单个或多个器件的情况。

Resume Command [A5h]

在一个典型应用中，要完成一次货币交易需要多次访问 DS1963S。如果执行主机/用户鉴别访问的次数还要增加。这意味着在多点环境中，每次访问都要重复执行 Match ROM 命令和发送 64 位 ROM 序列号。为了提高多点环境中的数据吞吐率，设置了 Resume Command（摘要命令）功能。该功能检测 RC 位的状态，如果置位，就直接传递控制给存储器和 SHA 功能，类似于 Skip ROM 命令。设置 RC 位的唯一方法是成功地执行 Match ROM，Search ROM 或 Overdrive Match ROM 命令。一旦设置了 RC 位，利用 Resume Command 功能就可重复访问同一器件。对于总线上另一器件的访问将清除 RC 位，以防两个或更多的器件同时响应 Resume Command 功能。

1-Wire 信令

为了保证数据的完整性，DS1963S 具有一个严格的信号协议。该协议在一条线上定义了四种类型的信号：包括复位脉冲和应答脉冲的复位序列，写 0，写 1 和读数据。除了应答脉冲以外，所有其它信号均由总线主控发出。DS1963S 能够以两种不同速度通信：常规速度和高速模式。如果没有明确设定为高速模式，DS1963S 就以常规速度通信。高速模式下，所有波形均采用快速定时。

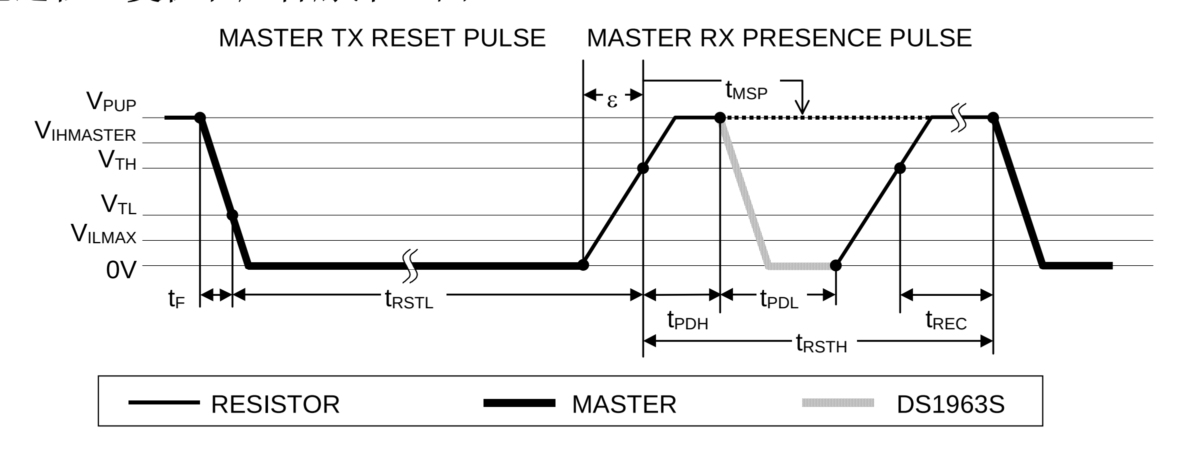
要使器件从空闲状态激活，1-Wire线上的电压需要从V_{PUP}降低到门限V_{TL}以下。要使器件从激活转换到空闲态，1-Wire线上的电压需要从V_{ILMAX}上升到越过门限值V_{TH}。V_{ILMAX}只被DS1963S参照用来判断逻辑电平，并不会触发任何事件。

启动与DS1963S之间的通信所需的初始化时序见图 11。复位脉冲后的应答脉冲表明DS1963S已经准备好接收数据、给出正确的ROM和存储器功能。在一个混合器件网络中，复位低电平时间t_{RSTL}需要足够长，以便最慢的 1-Wire从器件能够识别它。在标准速度下这个宽度为 480µs，高速模式下为 48µs。如果总线主控对下降沿进行了摆率控制的话，它必须拉低总线t_{RSTL} + t_F以补偿边沿的影响。如果t_{RSTL}等于或大于 480µs，总线上高速模式的器件就会退出高速模式回到标准模式。如果DS1963S处于高速模式而t_{RSTL}不大于 80µs，器件将保持高速模式。

主机释放总线后进入接收模式（RX）。此时，1-Wire总线被上拉电阻或DS2480B驱动器等有源电路拉升至V_{PUP}。当超过V_{TH}时，DS1963S等待t_{PDH}时间后将总线拉低t_{PDL}时间，发出一个应答脉冲。主机必须在t_{MSP}时刻监测 1-Wire总线逻辑状态来检测应答脉冲。

时间窗口t_{RSTH}至少等于t_{PDHMAX}，t_{PDLMAX}，与t_{RECMIN}之和。一旦t_{RSTH}到期，DS1963S即可开始数据通信。在一个混合器件网络中，t_{RSTH}在标准速度下应大于 480µs，高速模式应大于 48µs以适应其它的 1-Wire器件。

初始化过程（复位和应答脉冲） 图 11



读/写时隙

与 DS1963S 的数据通信基于时隙进行，每个时隙承载一位数据。写时隙由总线主机向从机传送数据。读时隙由从机向主机传送数据。有关读和写时隙的定义如图 12 所示。

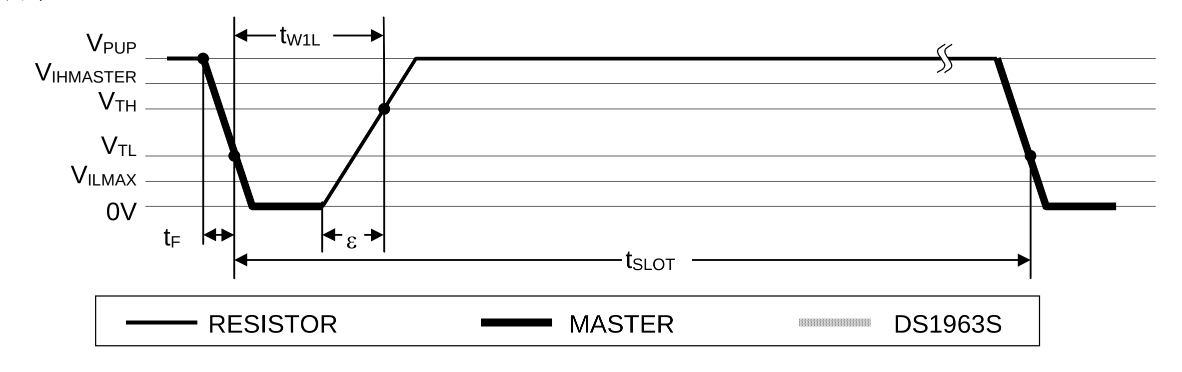
所有通信都从主机拉低数据线开始。随着 1-Wire线上的电压下降到门限V_{TL}以下，DS1963S启动其内部定时器以决定在写时隙何时采样数据线，以及在读时隙有效数据保持多长时间。

主机到从机

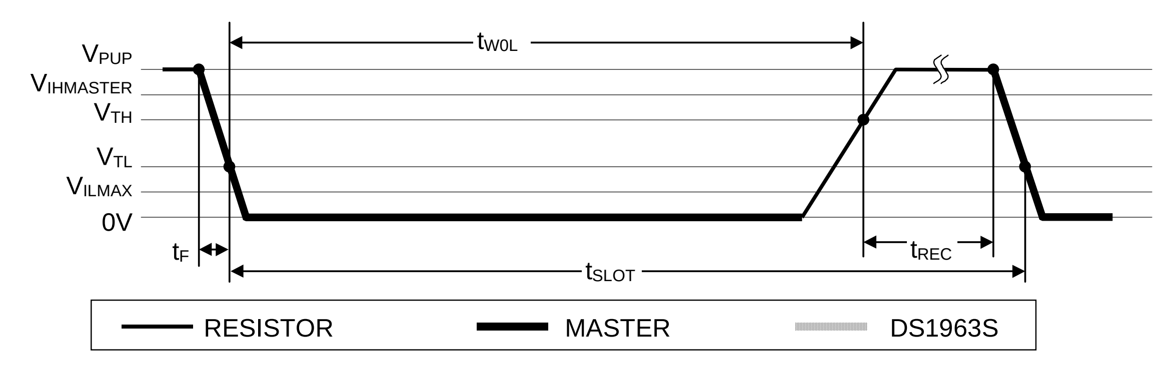
在写 **1** 时隙，数据线上的电压在写 1 低电平时间t_{W1LMAX}结束后必须已经达到V_{THMAX}门限。在写 **0** 时隙，数据线上的电压在写 0 低电平时间t_{W0LMIN}结束前必须一直保持低于V_{THMIN}门限。为实现最可靠的通信，数据线上的电压在整个t_{W0L}窗口都不能高于V_{ILMAX}。电压超过V_{THMAX}后，在准备好下一个时隙前DS1963S需要一个恢复时间t_{REC}。

读/写时隙图 图 12

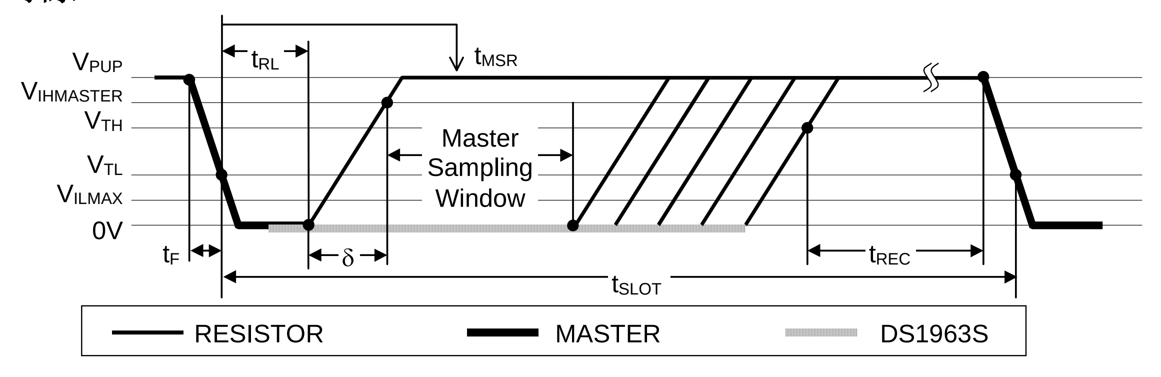
写 1 时隙



写 0 时隙



读数据时隙



从机到主机

读数据时隙非常接近于写 1 时隙。在读低时间t_{RL}结束前数据线上的电压必须一直低于V_{TLMIN}，在t_{RL}窗口内，发送 0 时，DS1963S将拉低数据线电压；其内部定时器决定何时结束拉低，电压重新开始升高。发送 1 时，DS1963S并不拉低数据线电压，t_{RL}一结束电压即开始升高。

主机采样窗口（t_{MSRMIN} + t_{MSRMAX}）一方面取决于t_{RL} + δ（上升时间），另一方面取决于DS1963S内部定时器。主机必须在采样窗口内采样数据线。为实现最可靠的通信 ，t_{RL}应该在允许的范围内尽可能短，主机采样时间必须接近但不能晚于t_{MSRMAX}。主机在读取数据线上的数据后应等待t_{SLOT}结束，以确保DS1963S在下一个时隙开始前有足够的恢复时间t_{REC}。

CRC 的生成

DS1963S有两种类型的CRC校验。其中一种CRC是 8 位的，在出厂时就已经计算好了，并用激光写入 64 位ROM的最高字节中。该CRC的等价多项式是$X^8 + X^5 + X^4 + 1$。为了确定ROM数据是否被无差错地读取，总线主控可用 64 位ROM的前 56 位计算CRC值，并将其与从DS1963S读来的值相比较。读ROM的时候，接收到的是 8 位CRC的原码形式（未求反的）。

另一类CRC是 16 位的，根据标准的CRC16 多项式$X^{16} + X^{15} + X^2 + 1$产生。该CRC用于读暂存器时检测执行Read Authenticated Page命令、Compute SHA功能时的错误，或用于写暂存器时快速检验数据传送的正确性。基于iButton的NV RAM在iButton扩展文件结构中进行差错检验时采用的是同一种CRC。与 8 位CRC不同的是，16 位CRC通常是以反码的形式发送或回送。DS1963S芯片内部的CRC发生器（图 13）用于在图 7 所示的命令流程中计算一个新的 16 位CRC。总线主控通过比较由器件读来的CRC和自己根据数据计算出的CRC，据此来决定是继续某一操作还是重读有CRC错误的数据部分。

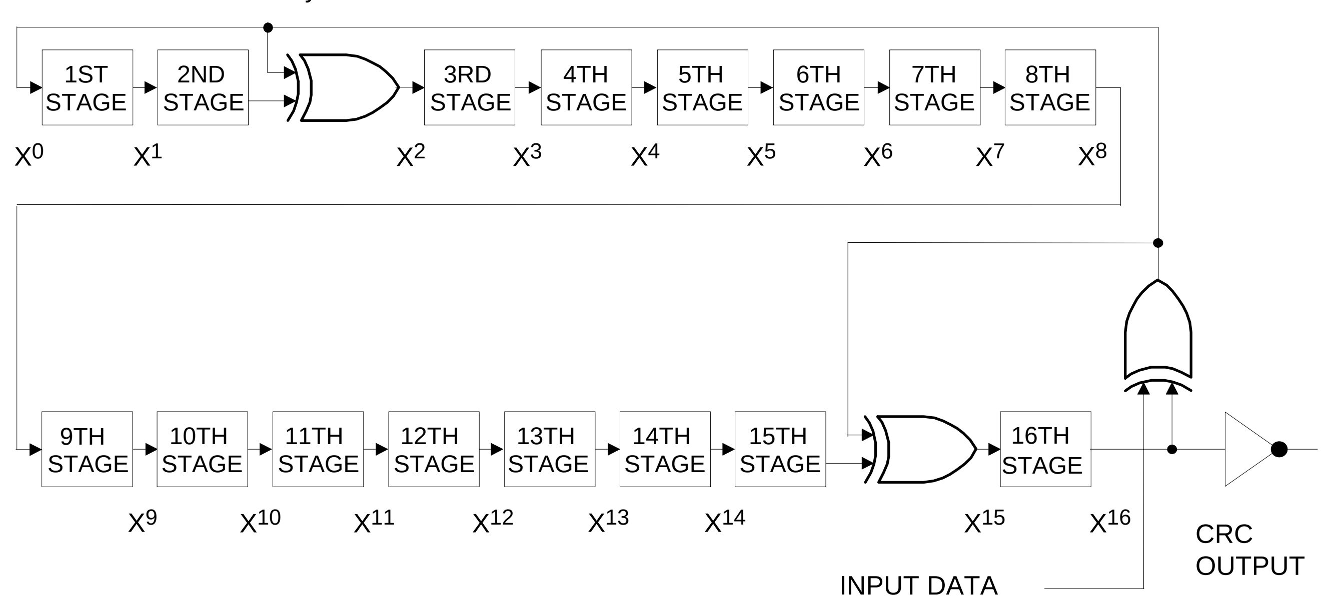
在 Write Scratchpad 命令中，CRC 校验码是通过首先清除 CRC 发生器，然后移入命令代码、目标地址 TA1 和 TA2 以及所有数据字节产生的。只有当暂存器的终止位置地址为 11111b 时 DS1963S 才发送该 CRC。数据可以从暂存器内的任意位置开始存放。CRC 的计算与 HIDE 标志位的状态无关。不过，HIDE 标志置位时，跟随在目标地址之后的数据字节仅用于计算 CRC，它们并不被暂存器接收。

在 Read Scratchpad 命令中，CRC 校验码是通过首先清空 CRC 发生器，然后移入命令代码、目的地址 TA1 和 TA2、E/S 字节以及由暂存器偏移地址开始的暂存器数据产生的。只有读到暂存器末尾的时候，DS1963S 才发送该 CRC 校验码，而与实际的终止位置地址无关。如果 HIDE 标志置位，计算 CRC 时暂存器数据由 FFh 字节取代，暂存器被隐蔽起来。

在 Read Authenticated Page 命令中，16 位 CRC 的计算首先是将命令字节移入清空的 CRC 发生器，随后是两个地址字节、数据字节、所寻址的存储页的写循环计数器及其相关密钥。写循环计数器由低字节开始移入。在进行 Compute SHA 操作时，CRC 计算首先是将命令字节移入清空的 CRC 发生器，随后是目标地址 TA1、TA2 和 SHA 控制字节。

关于产生CRC的详细资料，以及用硬件和软件实现的具体实例，参见*Book of DS19xx iButton Standards*。

CRC-16 硬件描述和多项式 图 13



物理规范

尺寸	见机械图
重量	3.3 克
预期寿命	见曲线
安全性	符合 UL#913 (第四版)标准；本质安全器件，经过 I 级，1 区，A、B、C、D 组指定区域的认证（申请中）

极限参数*

IO 对地电压	-0.5V, +6V
IO 吸收电流	20mA
温度范围	-40°C 至 +85°C
结温	+150°C
储存温度范围	-25°C 至 +50°C

* 这只是一个应力条件下的参数，并不意味着器件可以在符合或超出该规定所提及的工作条件下执行功能。长期暴露器件于极限条件会影响其可靠性。这些器件不应长期暴露于+70°C 以上的温度。

电气特性 (V_{PUP} = 2.8V至 5.25V, T_A = -40°C至+85°C)

参数	符号	条件	最小	典型	最大	单位	注释
通用数据 IO 口线							
1-Wire 上拉电阻	R_{PUP}				2.2	kΩ	1, 2
输入电容	C_{IO}			100	800	pF	3
输入负载电流	I_L	IO 口线 于V_{PUP}			9	µA	4
高电平至低电平切换门限	V_{TL}		0.7		2.9	V	5, 6, 7
输入低电平电压	V_{IL}				0.30	V	1, 5, 8
低平至高平切换门限	V_{TH}		0.6		2.9	V	5, 6, 9
4mA 时输出低电平电压	V_{OL}				0.4	V	5, 10
下降时间	t_F				5	µs	1
恢复时间	t_{REC}	标准速度, R_{PUP}=2.2kΩ	5			µs	1, 15
		高速模式, R_{PUP}=2.2kΩ	2				
		高速模式, 直接作用于复位脉冲之前; R_{PUP}=2.2kΩ	5				

参数	符号	条件	最小	典型	最大	单位	注释
时隙持续时间	t_{SLOT}	标准速度	69			μs	1, 15
		标准速度, -20°C 至+85°C	65				
		高速模式, V_{PUP} > 4.5V	8				
IO 口线, 1-Wire 复位, 在线检测周期							
复位低电平时间	t_{RSTL}	标准速度	540		960	μs	1, 14
		标准速度, -20°C 至+85°C	480		960		
		高速模式, V_{PUP} > 4.5V	48		80		
在线检测高电平时间	t_{PDH}	标准速度	17		60	μs	14
		高速模式, V_{PUP} > 4.5V	1.8		6		
在线检测低电平时间	t_{PDL}	标准速度	78		260	μs	14
		标准速度, -20°C 至+85°C	78		240		
		高速模式, V_{PUP} > 4.5V	7.7		24		
在线检测采样时间	t_{MSP}	标准速度	60		95	μs	1
		高速模式, V_{PUP} > 4.5V	6		9.5		
IO 口线, 1-Wire 写							
写 0 低电平时间	t_{W0L}	标准速度	64		120	μs	1, 14
		标准速度, -20°C 至+85°C	60		120		
		高速模式, V_{PUP} > 4.5V	6		15.4		
写 1 低电平时间	t_{W1L}	标准速度	5		15 - ε	μs	1, 11
		高速模式	1		2 - ε		
IO 口线, 1-Wire 读							
读低电平时间	t_{RL}	标准速度	5		15 - δ	μs	1, 12
		高速模式	1		2 - δ		
读采样时间	t_{MSR}	标准速度	$t_{RL} + \delta$		15	μs	1, 12
		高速模式	$t_{RL} + \delta$		2		
SHA-1 引擎							
计算时间	t_{SHA}			0.4	1.15	ms	
SHA-1 计算次数	N_{SHA}		(见图)			---	13

注释

1) 系统要求。
2) 最大允许的上拉电阻取决于系统中的 1-Wire 器件数量和 1-Wire 恢复时间。这里规定的数值适合于只有一个器件的系统和最小 1-Wire 恢复时间。对于负载较重的系统，可能需要 DS2480 那样的有源上拉。
3) 初次通电时，数据引脚上的电容可能达 800pF。如果用 2.2kΩ的电阻将数据线上拉到 V_{PUP}，那么在上电 2.5µs后，寄生电容不会影响到正常通信。
4) 输入负载到地。
5) 所有电压参照于地。
6) V_{TL}, V_{TH}与内部供电电压有关。
7) 低于此值的电压，在 IO 的下降沿检测到逻辑 0。
8) 无论何时主机拉低总线，IO上的电压都应低于或等于V_{ILMAX}。
9) 高于此值的电压，在 IO 的上升沿检测到逻辑 1。
10) 电压不高于 1V 时，I-V 特性呈线性。
11) ε为上拉电路将IO上的电压从V_{IL} 拉到V_{TH}需要的时间。
12) δ为上拉电路将IO上的电压从V_{IL}拉到总线主机的输入高门限所需的时间。
13) 使用内部能源可运行 SHA-1 计算的次数与器件的工作和存储温度有关。
14) 带阴影的参数不兼容于已发布的iButton标准。参见下面的对照表。
15) 为增加器件的寄生电源，恢复时间被有意从标准的 1µs 延长到更大值。这种变化改善了芯片的性能，但并不被视为对已发布标准的不兼容。

T_A = -40°C至+85°C时的不兼容项

参数名称	标准数值				**DS1963S 数值**			
	标准速度		高速		标准速度		高速	
	最小	最大	最小	最大	最小	最大	最小	最大
t_{SLOT} (包括 t_{REC})	61µs	(未定义)	7µs	(未定义)	69µs	(未定义)	8µs	(未定义)
t_{RSTL}	480µs	(未定义)	48µs	80µs	540µs	960µs	48µs	80µs
t_{PDH}	15µs	60µs	2µs	6µs	17µs	60µs	1.8µs	6µs
t_{PDL}	60µs	240µs	8µs	24µs	78µs	260µs	7.7µs	24µs
t_{W0L}	60µs	120µs	6µs	16µs	64µs	120µs	6µs	15.4µs
t_{SLS}, t_{SPD}	15µs	60µs	2µs	6µs	19µs	64µs	2µs	4.8µs

T_A = -20°C至+85°C 时的不兼容项

参数名称	标准数值				DS1963S 数值			
	标准速度		高速		标准速度		高速	
	最小	最大	最小	最大	最小	最大	最小	最大
t_{SLOT}	61µs	(未定义)	7µs	(未定义)	65µs	(未定义)	8µs	(未定义)
t_{RSTL}	480µs	(未定义)	48µs	80µs	480µs	960µs	48µs	80µs
t_{PDH}	15µs	60µs	2µs	6µs	17µs	60µs	1.8µs	6µs
t_{PDL}	60µs	240µs	8µs	24µs	78µs	240µs	7.7µs	24µs
t_{W0L}	60µs	120µs	6µs	16µs	60µs	120µs	6µs	15.4µs
t_{SLS}, t_{SPD}	15µs	60µs	2µs	6µs	19µs	60µs	2µs	4.8µs

预期寿命随温度的变化

